Our Ref.:
KOY-5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

- -x
In re Application of: :
T. Takeyama :

Serial No.: : 600 Third Avenue
New York, NY 10016

Filed: Concurrently herewith :

For: MEDICAL INFORMATION :
MANAGEMENT SYSTEM
:
- -x

September 8, 2003

Commissioner of Patents
P.O. BOX 1450
Alexandria VA 222313-1450

S i r :

With respect to the above-captioned application, Applicant(s) claim the priority of the attached application(s) as Provided by 35 U.S.C. 119.

Respectfully submitted,

Donald C. Lucas

MUSERLIAN, LUCAS AND MERCANTI
Attorneys for Applicants
600 Third Avenue
New York, NY 10016
(212) 661-8000

Enclosed: Certified Priority Document, Japanese Patent Application No. 2002-268710 filed September 13, 2002.

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　９月１３日

出願番号
Application Number:　特願２００２－２６８７１０

[ST.10/C]:　[ＪＰ２００２－２６８７１０]

出願人
Applicant(s):　コニカ株式会社

２００３年　６月１０日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０４５３３０

【書類名】　特許願
【整理番号】　DKY00767
【提出日】　平成14年 9月13日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 13/00
G06F 7/00
G06F 9/00　310
【発明者】
【住所又は居所】　東京都日野市さくら町１番地　コニカ株式会社内
【氏名】　竹山　敏久
【特許出願人】
【識別番号】　000001270
【氏名又は名称】　コニカ株式会社
【代理人】
【識別番号】　100090033
【弁理士】
【氏名又は名称】　荒船　博司
【手数料の表示】
【予納台帳番号】　027188
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　医療情報管理システム

【特許請求の範囲】

【請求項１】

データベースに医療情報を記憶する複数のデータベース装置と、統合的に医療情報を管理する管理装置と、前記データベース装置及び前記管理装置のうち少なくとも一方を操作する操作端末と、を備える医療情報管理システムにおいて、

データベース装置は、データベースに記憶された医療情報の中から必要な情報を抽出して前記管理装置に送信する自動送信手段を備え、

管理装置は、

前記自動送信手段から送信された医療情報を受信する受信手段と、

前記受信手段により受信された医療情報を、当該医療情報に含まれる所定の情報に基づいて統合的に記憶する記憶手段と、

前記操作端末の操作者が予め登録された個人であるか否かを照合して認証する個人照合手段と、

前記操作端末により操作指示された医療情報が操作可能な情報であるか否かを判別するデータアクセス権確認手段と、

を備えることを特徴とする医療情報管理システム。

【請求項２】

前記管理装置は、前記個人照合手段により認証された操作者からの操作指示に基づいて、前記データアクセス権確認手段により前記操作指示された医療情報が操作可能な情報であると判別された場合に、当該医療情報の閲覧、追加、修正及び加工のうち少なくとも１種の操作を行わせる制御手段を備えることを特徴とする請求項１記載の医療情報管理システム。

【請求項３】

医療情報を記録媒体に電子情報として記録又は印刷媒体にハードコピーとして出力する出力装置を備え、

前記管理装置は、前記操作端末により出力指示された医療情報が前記出力装置に出力可能な情報であるか否かを判別し、当該医療情報が出力可能な情報である

場合に、前記出力装置に医療情報を出力する出力許可手段を備えることを特徴とする請求項１又は２に記載の医療情報管理システム。

【請求項４】

前記管理装置は、前記制御手段により、前記記憶手段に記憶された医療情報に追加、修正又は加工の操作が行われた場合に、変更履歴を当該医療情報に対応付けて記憶手段に記憶させるデータ改竄防止手段を備えることを特徴とする請求項２項に記載の医療情報管理システム。

【請求項５】

前記管理装置は、前記制御手段により、前記記憶手段に記憶された医療情報に閲覧、追加、修正又は加工の操作が行われた場合に、当該医療情報が操作された日時を付帯情報として医療情報に付与する日時付与手段を備えることを特徴とする請求項２又は４記載の医療情報管理システム。

【請求項６】

前記日時付与手段は、前記自動送信手段により送信された医療情報が前記受信手段により受信された日時又は前記記憶手段に記憶された日時を付帯情報として当該医療情報に付与することを特徴とする請求項５記載の医療情報管理システム。

【請求項７】

前記自動送信手段は、送信する医療情報と、過去に送信した医療情報との差分を検出し、前記差分に対応する医療情報を抽出し、当該抽出された医療情報を必要な情報として管理装置に送信することを特徴とする請求項１記載の医療情報管理システム。

【請求項８】

前記自動送信手段により送信される医療情報は、当該医療情報が作成された作成日時を付帯情報として含み、

前記管理装置は、受信手段により受信した医療情報に含まれる作成日時と、記憶手段に記憶されている医療情報に含まれる作成日時とを比較して、受信手段により受信した医療情報のうち作成日時の異なる医療情報を記憶手段に記憶させる記憶制御手段を備えることを特徴とする請求項１記載の医療情報管理システム。

【請求項９】

前記個人照合手段は、パスワード、ＩＤカード、指紋、掌紋、声紋、顔、署名筆跡、虹彩パターン、眼底パターンあるいは静脈パターンに基づいて個人を照合する手段の中から選ばれる少なくとも１種の個人照合手段であることを特徴とする請求項１から４のいずれか一項に記載の医療情報管理システム。

【請求項１０】

前記個人照合手段は、パスワード又はＩＤカードを照合させる手段と、指紋、声紋あるいは虹彩パターンを照合させる手段の中から選ばれる少なくとも１種とを組み合わせた個人照合手段であることを特徴とする請求項９記載の医療情報管理システム。

【請求項１１】

前記制御手段により、閲覧、追加、修正又は加工される医療情報は、文字データ、オンオフデータ、静止画像データ、動画データの中から選ばれる少なくとも１種のデータであることを特徴とする請求項２記載の医療情報管理システム。

【請求項１２】

前記操作端末は、操作指示を入力するための入力手段を備え、

前記入力手段は、ペン入力、キーボード入力、マウス入力あるいは音声入力から選ばれる少なくとも１種の入力手段であることを特徴とする請求項１記載の医療情報管理システム。

【請求項１３】

前記医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも１種のデータを含むことを特徴とする請求項１から８又は１１のいずれか一項に記載の医療情報管理システム。

【請求項１４】

前記自動送信手段により送信される医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ

、介護保険システムデータ、医療関連文献データから選ばれる少なくとも１種のデータを含むことを特徴とする請求項１から８、１１又は１３のいずれか一項に記載の医療情報管理システム。

【請求項１５】

前記管理装置と前記操作端末は、ネットワークを介して接続され、当該ネットワークは、前記管理装置と前記操作端末とを接続するための専用回線により構築されていることを特徴とする請求項１記載の医療情報管理システム。

【請求項１６】

前記管理装置は、

前記操作端末に送信する情報を暗号化して送信する暗号化送信手段と、

前記操作端末から送信された情報を受信して復号化する復号化受信手段と、

前記操作端末は、

前記管理装置に送信する情報を暗号化して送信する暗号化送信手段と、

前記管理装置から送信された情報を受信して復号化する復号化受信手段と、

を備えることを特徴とする請求項１又は１５に記載の医療情報管理システム。

【請求項１７】

前記管理手段の記憶手段は、医療情報の種類に応じて情報を記憶する複数のデータベースから構成され、

前記制御手段は、操作端末からの操作指示に応じて前記複数のデータベースから対応する医療情報を読み出して、閲覧、追加、修正及び加工のうち少なくとも１つの操作を制御することを特徴とする請求項２記載の医療情報管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、医療情報管理システムに関する。

【０００２】

【従来の技術】

近年、医療の効率化が求められている中で、院内外のネットワーク化、システム化が進んでおり、病院情報システム（ＨＩＳ）、放射線科情報システム（ＲＩ

Ｓ）、画像保存転送システム（ＰＡＣＳ）、電子カルテ、遠隔医療などを有機的に連携させるトータルシステムとしてのニーズも大きくなってきている。さらに、地域医療を効率的に行うために医療機関間でのデータの共有化も徐々に進行してきており、これにより患者の重複した検査や治療、薬の投与などが避けられるようになってきた。

【０００３】

ところで、種々のデータをネットワークで接続されるようになってくると、患者の個人情報の漏洩に対するセキュリティの問題、また、種々のデータがデジタルデータとして保管されているために、データの人為的な改ざん防止の問題などについても課題となる場合がある。

【０００４】

電子商取引などで採用しているデジタル署名や電子署名など、日本では「電子署名及び認証業務に関する法律」、米国では「グローバルな商取引と国内商取引における電子署名法」、欧州では「電子署名のための共同体の枠組みに関する指令」等の法律あるいは指令として出され、個人を特定することに関しての取り組みが成されている。また、インターネット上では、例えばＷｅｂ標準化団体、Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ　Ｃｏｎｓｏｒｔｉｕｍ（Ｗ３Ｃ）からＸＭＬベースの電子署名技術の推奨規格などが提案されている。

【０００５】

医療分野においても、例えば、患者に対して指紋照合による確認手段（例えば、特許文献１，２参照）や、医療機関への来訪者、医療機関に出入する医療機関関係者又は医療機関内で出生した新生児に対して虹彩照合による確認手段（例えば、特許文献３，４参照）や、患者に対して声紋照合による確認手段（例えば、特許文献５，６参照）を導入することが提案されている。さらに、上述した各データへのアクセス可能な医療スタッフを予め制限するような試みがなされている（例えば、特許文献７～９参照）。

【０００６】

【特許文献１】

特開２０００－１５５７８２号公報

【特許文献２】

特開２００１－３１２５６６号公報

【特許文献３】

特開２０００－２４２７８８号公報

【特許文献４】

特開２００１－７６０７２号公報

【特許文献５】

特開平８－７１１４８号公報

【特許文献６】

読会平１０－２０１８２７号公報

【特許文献７】

特開２００２－４１６５６号公報

【特許文献８】

特開２００２－８２８３９号公報

【特許文献９】

特開２００２－１８３３１９号公報

【０００７】

【発明が解決しようとする課題】

しかしながら、近年の医療情報のネットワーク化やインターネットによる広域利用が行われた場合、医療事故の問題、さらにはデータに記載されている情報が個人のプライバシーに関わるといった問題等が生じるため、種々の観点からセキュリティに関する要望がより高くなってきている。

【０００８】

本発明は、上記の課題を鑑みてなされたものであり、本発明の目的は、種々の医療情報が記憶されるデータベースに対するセキュリティを考慮した医療情報管理システムを提供することにあり、さらに詳しくは個人照合手段により識別された個人情報に基づいて提供される医療情報を管理する医療情報管理システムを提供することである。

【０００９】

【課題を解決するための手段】

本発明の目的は、以下の構成により達成された。

【００１０】

上記課題を解決するために、請求項１記載の発明は、

データベースに医療情報を記憶する複数のデータベース装置と、統合的に医療情報を管理する管理装置と、前記データベース装置及び前記管理装置のうち少なくとも一方を操作する操作端末と、を備える医療情報管理システムにおいて、

データベース装置は、データベースに記憶された医療情報の中から必要な情報を抽出して前記管理装置に送信する自動送信手段を備え、

管理装置は、

前記自動送信手段から送信された医療情報を受信する受信手段と、

前記受信手段により受信された医療情報を、当該医療情報に含まれる所定の情報に基づいて統合的に記憶する記憶手段と、

前記操作端末の操作者が予め登録された個人であるか否かを照合して認証する個人照合手段と、

前記操作端末により操作指示された医療情報が操作可能な情報であるか否かを判別するデータアクセス権確認手段と、

を備えることを特徴としている。

【００１１】

請求項２記載の発明は、請求項１記載の医療情報管理システムにおいて、

前記管理装置は、前記個人照合手段により認証された操作者からの操作指示に基づいて、前記データアクセス権確認手段により前記操作指示された医療情報が操作可能な情報であると判別された場合に、当該医療情報の閲覧、追加、修正及び加工のうち少なくとも１種の操作を行わせる制御手段を備えることを特徴としている。

【００１２】

請求項３記載の発明は、請求項１又は２に記載の医療情報管理システムにおいて、

医療情報を記録媒体に電子情報として記録又は印刷媒体にハードコピーとして

出力する出力装置を備え、

前記管理装置は、前記操作端末により出力指示された医療情報が前記出力装置に出力可能な情報であるか否かを判別し、当該医療情報が出力可能な情報である場合に、前記出力装置に医療情報を出力する出力許可手段を備えることを特徴としている。

【００１３】

請求項４記載の発明は、請求項２記載の医療情報管理システムにおいて、

前記管理装置は、前記制御手段により、前記記憶手段に記憶された医療情報に追加、修正又は加工の操作が行われた場合に、変更履歴を当該医療情報に対応付けて記憶手段に記憶させるデータ改竄防止手段を備えることを特徴としている。

【００１４】

請求項５記載の発明は、請求項１から４のいずれか一項に記載の医療情報管理システムにおいて、

前記管理装置は、前記制御手段の操作制御により、前記記憶手段に記憶された医療情報に閲覧、追加、修正又は加工の操作が行われた場合に、当該医療情報が操作された日時を付帯情報として医療情報に付与する日時付与手段を備えることを特徴としている。

【００１５】

請求項６記載の発明は、請求項５記載の医療情報管理システムにおいて、

前記日時付与手段は、前記自動送信手段により送信された医療情報が、前記受信手段により受信された日時又は前記記憶手段に記憶された日時を付帯情報として当該医療情報に付与することを特徴としている。

【００１６】

請求項７記載の発明は、請求項１記載の医療情報管理システムにおいて、

前記自動送信手段は、送信する医療情報と、過去に送信した医療情報との差分を検出し、前記差分に対応する医療情報を抽出し、当該抽出された医療情報を必要な情報として管理装置に送信することを特徴としている。

【００１７】

請求項８記載の発明は、請求項１記載の医療情報管理システムにおいて、

前記自動送信手段により送信される医療情報は、当該医療情報が作成された作成日時を付帯情報として含み、

前記管理装置は、受信手段により受信した医療情報に含まれる作成日時と、記憶手段に記憶されている医療情報に含まれる作成日時とを比較して、受信手段により受信した医療情報のうち作成日時の異なる医療情報を記憶手段に記憶させる記憶制御手段を備えることを特徴としている。

【００１８】

請求項９記載の発明は、請求項１から４のいずれか一項に記載の医療情報管理システムにおいて、

前記個人照合手段は、パスワード、ＩＤカード、指紋、掌紋、声紋、顔、署名筆跡、虹彩パターン、眼底パターンあるいは静脈パターンに基づいて個人を照合させる手段の中から選ばれる少なくとも１種の個人照合手段であることを特徴としている。

【００１９】

請求項１０記載の発明は、請求項９記載の医療情報管理システムにおいて、

前記個人照合手段は、パスワード又はＩＤカードを照合させる手段と、指紋、声紋あるいは虹彩パターンを照合させる手段の中から選ばれる少なくとも１種とを組み合わせた個人照合手段であることを特徴としている。

【００２０】

請求項１１記載の発明は、請求項２記載の医療情報管理システムにおいて、

前記制御手段により、閲覧、追加、修正又は加工される医療情報は、文字データ、オンオフデータ、静止画像データ、動画データの中から選ばれる少なくとも１種のデータであることを特徴としている。

【００２１】

請求項１２記載の発明は、請求項１記載の医療情報管理システムにおいて、

前記操作端末は、操作指示を入力するための入力手段を備え、

前記入力手段は、ペン入力、キーボード入力、マウス入力あるいは音声入力から選ばれる少なくとも１種の入力手段であることを特徴とする。

【００２２】

請求項１３記載の発明は、請求項１から８又は１１のいずれか一項に記載の医療情報管理システムにおいて、

前記医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも１種のデータを含むことを特徴としている。

【００２３】

請求項１４記載の発明は、請求項１から８、１１又は１３のいずれか一項に記載の医療情報管理システムにおいて、

前記自動送信手段により送信される医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも１種のデータを含むことを特徴としている。

【００２４】

請求項１５記載の発明は、請求項１記載の医療情報管理システムにおいて、

前記管理装置と前記操作端末は、ネットワークを介して接続され、当該ネットワークは、前記管理装置と前記操作端末とを接続するための専用回線により構築されていることを特徴としている。

【００２５】

請求項１６記載の発明は、請求項１又は１５に記載の医療情報管理システムにおいて、

前記管理装置は、

前記操作端末に送信する情報を暗号化して送信する暗号化送信手段と、

前記操作端末から送信された情報を受信して復号化する復号化受信手段と、

前記操作端末は、

前記管理装置に送信する情報を暗号化して送信する暗号化送信手段と、

前記管理装置から送信された情報を受信して復号化する復号化受信手段と、

を備えることを特徴としている。

【００２６】

請求項１７記載の発明は、請求項２記載の医療情報管理システムにおいて、

前記管理手段の記憶手段は、医療情報の種類に応じて情報を記憶する複数のデータベースから構成され、

前記制御手段は、操作端末からの操作指示に応じて前記複数のデータベースから医療情報を読み出して、閲覧、追加、修正及び加工のうち少なくとも１つの操作を制御することを特徴としている。

【００２７】

【発明の実施形態】

以下、図１～１９を参照して本発明の実施の形態を詳細に説明する。ただし、発明の範囲は、図示例に限定されない。

【００２８】

ここで、本発明における医療情報管理システムと、本第１から第７の実施の形態における医療情報管理システム１００とにおける各構成要素の対応関係を明示する。すなわち、本発明における管理装置は、本実施の形態の医療情報統括管理サーバ１ａ～１ｇに対応し、本発明のデータベース装置は、本実施の形態の医療情報データベース２～８に対応している。本発明の操作端末は、本実施の形態の操作端末Ａ～Ｅ、操作端末２０～８０に対応し、本発明の出力装置は、本実施の形態の出力装置ｘ～ｚに対応している。

【００２９】

また、本発明の管理装置と、本実施の形態の医療情報統括管理サーバ１ａ～１ｇの各構成要素の対応関係を明示すると、本発明の受信手段は、本実施の形態の受信手段１５に対応し、本発明の記憶手段は、本実施の形態のデータベース１６に対応する。また、本発明の個人照合手段は、本実施の形態の個人照合手段１２に対応し、本発明のデータアクセス権確認手段は、本実施の形態のデータアクセス権確認手段１３に対応している。また、本発明の制御手段、記録制御手段は、本実施の形態の制御部１１に対応し、本発明の出力許可手段は、本実施の形態の出力許可手段１４に対応している。さらに、本発明のデータ改竄防止手段は、本

実施の形態のデータ改竄防止手段１７に対応し、本発明の日時付与手段は、本実施の形態の日付日時付与手段１８に対応している。また、本発明のデータベース装置の自動送信手段は、本実施の形態の医療情報データベース２～６の自動送信手段２１～６１に対応している。

【００３０】

まず、本実施の形態の構成を説明する。

図１は、例えば一つの医療機関内において、医療情報統括管理サーバ１により医療情報を一元管理する医療情報管理システム１００のシステム構成を示す概念図である。図１に示すように、医療情報統括管理サーバ（以下、「管理サーバ」と省略する）１と、この管理サーバ１を操作する端末である操作端末Ａ～Ｅと、医療情報データベース２～８まで７種のデータベース（以下、「ＤＢ」と省略する）と、各医療情報ＤＢ２～８を操作する端末である操作端末２０～８０とが設けられている。なお、ここで言う操作する端末とはデータベースに記憶される医療情報の閲覧、追加、修正及び加工することのできるものを指す。

【００３１】

管理サーバ１は、医療情報を一元管理するための装置であり、ネットワークＬを介して接続された操作端末Ａ～Ｅにより、データベース１６に記憶される医療情報の閲覧、追加、修正及び加工することができる。医療情報ＤＢ２～８は、管理サーバ１にネットワークＬを介して接続されており、操作端末２０～８０により、データベースに記憶される医療情報を閲覧、追加、修正及び加工することができる。また、医療情報ＤＢ２～８に接続された操作端末２０～８０により、管理サーバ１にアクセスして医療情報の閲覧、追加、修正及び加工が可能となっている。

【００３２】

ここで、ネットワークＬは、サーバと、複数のク操作端末とを接続して構成され、接続されたサーバ及び複数の操作端末間で情報や資源（例えば、データベース、出力装置等）を共有するための、限られたエリア内におけるネットワークである。例えば、ＷＷＷ（ワールド・ワイド・ウェブ）やＴＣＰ／ＩＰなどの、インターネットで普及している技術を使ってネットワークＬを構築することにより

、信頼性の高いネットワークをスピーディに構築できるとともに、インターネットとの親和性を高めることができる。なお、ネットワークＬは、情報管理の信頼性の観点から、特定のユーザのみアクセス可能なセキュリティを確保しているネットワークであることが望ましい。

【００３３】

なお、図１では７個の医療情報ＤＢ２～８を一例として示したが、医療情報ＤＢは２個以上であれば特に制限はなく、医療情報ＤＢ２～８に接続されている操作端末２０～８０についても、図１では一つのみ備える構成として記載したが２個以上又は複数個設置しても良い。また、管理サーバ１に接続された操作端末Ａ～Ｅを５個として記載したが、管理サーバ１を操作する端末として各種医療情報ＤＢ２～８に接続された操作端末２０～８０で代用しても良いし、直接バス等により接続された端末を１個あるいは２個以上備える構成であっても良い。

【００３４】

図２は、図１同様に医療情報を一元管理している医療情報管理システム２００のシステム構成の一例を示す図である。この医療情報管理システム２００は、地域医療情報化を目的とするものであり、各種医療機関Ａ～Ｇで運用されているデータベースがネットワークＮにより接続され、医療情報統括管理サーバ（以下、「管理サーバ」と記す）１ｂにより一元管理されている。図２に示すように、それぞれの医療機関Ａ～Ｇに備えられるの７種のデータベースが有り、この医療機関ＤＢａ～ｇを操作する操作端末ａ１～ｇ１が設けられている。なお、ここで言う操作する端末とはデータベースの医療情報を閲覧、追加、修正及び加工できるものであり、例えば、医療機関ＤＢａを操作する操作端末としては操作端末ａ１、操作端末ａ２、操作端末ａ３……操作端末ａＮのように複数個設置してあっても良い。

【００３５】

管理サーバ２は、医療情報管理システム２００の医療情報を一元管理するための装置であり、管理サーバ２に接続された操作端末α～εの操作により、医療情報の閲覧、追加、修正及び加工が可能となっている。また、医療機関ＤＢａ～ｇは、管理サーバ２にネットワークＮを介して接続され、操作端末ａＮ～ｇＮの操

作により、管理サーバ２にアクセスして、医療情報の閲覧、追加、修正及び加工が可能となっている。

【００３６】

ここで、ネットワークＮは、電話回線網、ＩＳＤＮ回線網、専用線、移動体通信網、通信衛星回線、ＣＡＴＶ回線網等の各種通信回線と、それらを接続するインターネットサービスプロバイダ基地局等を含む。なお、ネットワークＮは、任意な時に接続が可能であればよく、常時接続されている必要はない。また、ネットワークＮは、情報管理の信頼性の観点から、特定のユーザのみアクセス可能なセキュリティを確保しているネットワークであることが望ましい。特に、管理サーバ２と管理サーバ２を操作する操作端末α～εとの接続は、専用回線により構築されていることが好ましい。操作端末α～εは、管理サーバ２の医療情報を直接操作可能な端末だからである。

【００３７】

なお、操作端末ａＮ～操作端末ｇＮは、前記管理サーバ２にアクセスして、医療情報の追加、変更、閲覧が可能な操作端末としても良い。また、図２では医療機関ＤＢａ～ｇを７個備える場合を例として記載したが、２個以上であれば特に制限はない。また、管理サーバ２にネットワークＮを接続された操作端末α～εを５個備える場合を例として記載したが、管理サーバ２を操作する端末として各種医療機関Ａ～Ｇの各ＤＢに接続された操作端末ａＮ～ｇＮを代用しても良く、直接接続された端末が１個又は２個以上であっても良い。

【００３８】

以上、２つの医療情報管理システムのシステム構成について説明を行ったが、上述した医療情報管理システム１００，２００は一例であり、その他種々の形態により構成されていても良い。なお、医療情報管理システム１００を構成する各部と、医療情報管理システム２００を構成する各部は、略同一の構成及び動作によってなるため、以下では、医療情報管理システム１００に本発明が適用された場合を例として第１から第７の実施の形態について説明を行う。

【００３９】

［第１の実施の形態］

まず、医療情報管理システム１００における管理サーバ１ａについて説明する。図３は、医療情報管理システム１００における管理サーバ１ａの要部構成を示すブロック図である。なお、図３では、本第１の実施の形態に必要な構成のみを示し、説明に不要なその他の構成及び装置については省略している。

【００４０】

図３に示すように、管理サーバ１ａは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、出力許可手段１４、受信手段１５、データベース１６等を備えて構成されており、各部はバスにより接続されている。また、管理サーバ１ａは、ネットワークＬを介して接続される、管理サーバ１ａを操作するための操作端末Ａ～Ｅ及び管理サーバ１ａ内の医療情報をハードコピーとして出力するための出力装置ｘ～ｚを備えている。

【００４１】

制御部１１は、データベース１６内の記憶装置（図示せず）に記憶されている各種システムプログラムを読み出して実行し、管理サーバ１の各部を駆動制御する。具体的に、制御部１１は、後述する情報蓄積処理１（図４参照）、情報利用処理１（図５参照）を実行する。この情報蓄積処理１を実行するに際して、制御部１１は、医療情報ＤＢ２～６から送信される医療情報を受信すると、受信した医療情報から患者情報を抽出して、データベース１６内で同一の患者に関する医療情報があるかを検索する。そして、データベース１６内に同一の患者に関する医療情報がある場合、受信した医療情報を患者情報に対応付けて、既に記憶されている医療情報と統合してデータベース１６に記憶させる。

【００４２】

また、情報利用処理１を実行するに際して、制御部１１は、操作端末Ａ～Ｅからアクセス要求が送信されると、アクセス要求に含まれる操作端末Ａ～Ｅの操作者の個人情報を抽出して、個人照合手段１２により個人認証を行わせる。個人認証が成功した場合、データアクセス権確認手段１３により指示された医療情報が利用可能な情報であるかを確認させ、当該医療情報が利用可能な情報である場合、医療情報の閲覧、追加、修正又は加工等を行わせる。さらに、操作端末Ａ～Ｅから医療情報を出力する指示が入力された場合、制御部１１は、出力許可手段１

５により、指示された医療情報が出力可能な情報であるかを確認させ、当該医療情報が出力可能な情報である場合、出力許可手段１５を介して出力装置ｘ～ｚに出力させる。

【００４３】

個人照合手段１２は、操作端末Ａ～ＥからネットワークＮを介して送信されたアクセス要求を受信する。また、操作端末Ａ～Ｅを操作する操作者の個人情報をアクセス要求から取得して、この個人情報に基づいて操作端末Ａ～Ｅの操作者がアクセス可能な操作者であるかを判別する。ここで、個人情報は、個人を特定するための情報として、パスワード、ＩＤカード情報、指紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターンあるいは静脈（血管）パターン等を含んでおり、予めデータベース１６にアクセス可能な操作者として登録されている個人情報と比較して、個人の認証を行う。

【００４４】

個人照合手段１２は、パスワード、ＩＤカード、指紋、掌紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターンあるいは静脈（血管）パターンを照合させる手段の中から選ばれる少なくとも１種の個人照合手段であることが好ましく、この中で指紋、声紋あるいは虹彩パターンのように個人特有の情報を照合させる手段がセキュリティの面からより好ましい。また、さらにセキュリティを向上させるためには個人照合手段１２としてパスワードまたはＩＤカードによる認証と、指紋、声紋あるいは虹彩パターンを照合させる手段の中から選ばれる少なくとも１種の認証とを組み合わせた個人照合手段であることがより好ましい。

【００４５】

これにより、種々の情報に基づいて操作者の個人認証を確実に行うことができ、医療情報管理システムのセキュリティを向上することができる。あるいは、複数の個人照合手段を組み合わせることにより、第３者による不正なシステムへの進入を確実に防ぐことができる。また、種々の個人照合手段を適用可能にすることにより汎用性の高いシステムを提供することができる。

【００４６】

なお、アクセス可能な操作者としては、各種医療機関にいる医師、放射線技師、看護婦、薬剤師、病院の会計などを行う病院関係者、栄養士、訪問介護等を行うヘルパーあるいは患者等であり、管理サーバ１ａに蓄積された医療情報を必要とする者の中から任意に登録することができる。なお、個人照合手段１２は、個人照合するための装置を操作端末Ａ～Ｅに備えることにより、管理サーバ１に接続される前に操作端末Ａ～Ｅの個人照合手段１２により個人認証される構成であってもよい。この場合、データアクセス権確認手段に受信手段を備える構成とし、操作端末Ａ～Ｅの個人照合手段１２で認証特定された操作者の指示により、操作端末Ａ～Ｅから直接データアクセス権確認手段にアクセス要求が送信されても良い。

【００４７】

データアクセス権確認手段１３は、データベース１６に記憶されている医療情報のうち、閲覧、追加、修正あるいは加工が許可されている医療情報を識別する。ここで、閲覧、追加、修正あるいは加工できる医療情報としては、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システム、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータおよび医療関連文献データから選ばれる少なくとも１種のデータであり、より好ましくは前述のデータの中から選ばれる２種以上のデータである。

【００４８】

データアクセス権確認手段１３は、個人照合手段１２により取得された操作者の個人情報に基づいてアクセス可能な医療情報を識別する構成であっても良く、例えば、医師、放射線技師、看護婦、薬剤師および病院の会計などを行う病院関係者のみが操作者である場合においては、アクセス可能な医療情報として、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、および薬歴管理システムデータの中から選ばれる２種以上のデータであることがより好ましい。

【００４９】

また、個人照合手段１２により個人認証された操作者が、閲覧、追加、修正あ

るいは加工できるデータの種類としては、文字データ、オンオフデータ、静止画像データ、動画データの中から選ばれる少なくとも１種のデータであることが好ましい。また、この中で追加、修正あるいは加工できるデータが文字データあるいはオンオフデータである場合、操作端末Ａ～Ｅに備えられる入力手段（図示せず）は、ペン入力、キーボード入力、マウス入力あるいは音声入力から選ばれる少なくとも１種の入力手段であり、操作端末Ａ～Ｅを操作する者の習熟度によって適宜選択して用いることができる。なお、オンオフデータとは、情報をオン／オフにより示すデータであり、例えば、二者択一の情報である性別や病歴の有無等を示すデータである。

【００５０】

出力許可手段１４は、管理サーバ１内の医療情報を別の記録媒体に電子情報として記録あるいは医療情報を印刷媒体にハードコピーとして出力することを許可するか否かを、前記個人照合手段１２で得られた個人情報や、データアクセス権確認手段１３の判別結果に基づいて判別する。

【００５１】

受信手段１５は、複数の医療情報ＤＢ２～６の自動送信手段２１～６１から送信される医療情報を受信する。なお、自動送信手段２１～６１から送信される医療情報については、後述して詳細を説明する。

【００５２】

データベース１６は、プログラムやデータ等があらかじめ記憶されている記録媒体（図示せず）を有しており、この記録媒体は磁気的、光学的記録媒体、若しくは半導体メモリで構成されている。この記録媒体はデータベース１６に固定的に設けられるもの、若しくは着脱自在に装着するものであり、この記録媒体には、システムプログラム、当該システムに対応する各種処理プログラム、及び各種処理プログラムで処理されたデータ等を記憶する。プログラムは、コンピュータが読み取り可能なプログラムコードの形態で格納され、制御部１１は、当該プログラムコードに従った動作を逐次実行する。

【００５３】

また、記録媒体に記憶するプログラム、データ等は、その一部若しくは全部を

サーバやクライアント等の他の機器からＷＡＮ、ＬＡＮ等のネットワーク回線の伝送媒体を介して受信手段１５から受信して記憶する構成にしてもよく、さらに、記録媒体はネットワーク上に構築されたサーバの記録媒体であってもよい。また、前記プログラムをネットワーク回線等の伝送媒体を介してサーバやクライアントへ伝送してこれらの機器にインストールするように構成してもよい。

【００５４】

具体的に、データベース１６は、医療情報ＤＢ２～６から送信された医療情報を記憶しており、例えば、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータ、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データ等を含んでいる。これらの医療情報は、医療情報ＤＢ２～６から送信される医療情報に付帯する患者情報に基づいて、患者毎に統合されて管理、蓄積されている。この患者情報は、患者を特定できる情報として、氏名、年齢、住所等の保険証に記載された情報のほかに、指紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターン、静脈（血管）パターン、歯科情報等を含んでいる。また、データベース１６に記憶される医療情報に、追加、修正あるいは加工が行われた場合は、その操作結果を記憶する。

【００５５】

また、データベース１６は、管理サーバ１ａにアクセス可能な操作者として登録されている個人の個人情報を記憶している。この個人情報には、個人を特定するための情報として、パスワード、ＩＤカード情報、指紋、声紋、顔（輪郭等）、署名筆跡、虹彩パターン、眼底パターンあるいは静脈（血管）パターン等を含み、個人照合手段１２により、管理サーバ１ａにアクセス要求を送信した操作端末Ａ～Ｅの操作者の認証を行う際に利用される。

【００５６】

端末装置Ａ～Ｅは、ネットワークＮを介して管理サーバ１に接続され、管理サーバ１に記憶される医療情報の閲覧、追加、修正あるいは加工をするための操作指示を含むアクセス要求を管理サーバ１に送信する。このアクセス要求には、操作者の個人認証を行うための個人情報を含んでおり、この個人情報に基づいて操

作者がアクセス可能な個人であるか否かが認証される。そして、認証に成功した場合、操作指示が受け付けられる構成となっている。また、端末装置Ａ～Ｅは、医療情報を出力装置ｘ～ｚから出力させるための出力指示を管理サーバ１に送信する。

【００５７】

出力装置ｘ～ｚは、ネットワークＬを介して、管理サーバ１、端末装置Ａ～Ｅと接続されている。この出力装置ｘ～ｚは、例えば、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ハードディスク、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ、特開２００２－８３４３１号公報、特開２００２－１２３９４８号公報、特開２００２－１２３９４９号公報、特開２００２－１８３９７５号公報等に記載されている装置に用いられる高容量のホログラムメディア等への記録媒体への出力、サーマル銀塩記録メディア、フォトサーマル銀塩記録メディア、熱拡散性色素転写メディア、インクジェットメディアあるいは電子写真方式に用いられる記録メディア等の可視化情報やハードコピーとしての出力装置を適時選択して用いることができる。

【００５８】

次に、医療情報ＤＢ２～６について説明する。

医療情報ＤＢ２～６（以下、統括的に「医療情報ＤＢ２」として示す）は、操作端末２０～６０（以下、統括的に「操作端末２０」として示す）により操作され、操作端末２０の入力部（図示せず）を介して入力された医療情報のうち、必要な情報を管理サーバ１ａに自動で送信する自動送信手段２１～６１（以下、統括的に「自動送信手段２１」として示す）を備えている。

【００５９】

具体的に、この自動送信手段２１により管理サーバ１ａに送信される医療情報は、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システム、薬歴管理システムデータ、医薬品文書データ、介護保険システムデータ、医療関連文献データから選ばれる少なくとも１種のデータであり、より好ましくは前述のデータの中から選ばれる２種以上のデータである。さらに、医師、放射線技師、看護婦、薬剤師

および病院の会計などを行う病院関係者のみが使用する場合においては、臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータおよび薬歴管理システムデータから選ばれる２種以上のデータであることがより好ましい。

【００６０】

また、自動送信手段２１は、端末装置２０を介して入力され、医療情報ＤＢ２に蓄積された医療情報を自動的に管理サーバ１に送信して蓄積させるが、この際、管理サーバ１ａにおけるデータ処理を簡便にする目的で、送信される医療情報のうち、過去に管理サーバ１へ送信された医療情報との差分を検出し、追加または変更されている医療情報のみを管理サーバ１へ送信する。例えば、図３に示すように、医療情報ＤＢ２においては、データベースに記憶されている医療情報として、ａ１＋ｂ１が示されているが、そのうち必要な情報としてａ１のみがネットワークを介して管理サーバ１ａに送信される。また、他の医療情報ＤＢ３～６における医療情報ａ３～ａ６についても同様にネットワークを介して管理サーバ１に送信され、医療情報が蓄積される。

【００６１】

また、自動送信手段２１は、管理サーバ１ａへ医療情報を送信してデータベース１６に蓄積させる際に、送信する医療情報に情報を作成した作成日時を付帯情報として付与する構成であっても良い。これにより、管理サーバ１ａの制御部１１は、送信された医療情報の作成日時と、前回の送信され蓄積されている医療情報の作成日時とを照合し、新たに追加または変更されている医療情報のみをデータベース１６に蓄積させることができ、情報処理を簡便に行うことができる。

【００６２】

なお、自動送信手段２１により、医療情報ＤＢ２から管理サーバ１ａに医療情報が送信される時間は、個々のデータベースを構成するサーバやバックアップなどのシステム構成によって異なるが、医療情報ＤＢ２の使用頻度が少ない時間帯、例えば深夜から早朝に掛けて送信するのが好ましい。

【００６３】

端末装置２０は、医療情報ＤＢ２を操作するための端末であり、医療情報ＤＢ

２に記憶される医療情報の閲覧、追加、修正及び加工を行う装置である。また、端末装置２０は、ネットワークＮを介して管理サーバ１ａに接続されており、管理サーバ１ａに記憶される医療情報の閲覧、追加、修正及び加工を行うことも可能である。この場合も、端末装置２０はアクセス要求と共に、操作者の個人情報を管理サーバ１ａに送信し、認証が成功した場合に、アクセス要求が受け付けられる構成となっている。

【００６４】

次に、本第１の実施の形態における動作について説明する。

動作説明の前提として、以下のフローチャートに記述されている各処理を実現するためのプログラムは、コンピュータが読み取り可能なプログラムコードの形態でデータベース１６に格納されており、制御部１１は、当該プログラムコードに従った動作を逐次実行する。また、制御部１１は、伝送媒体を介して外部から供給されるプログラム及びデータを利用して、本実施の形態特有の動作を逐次実行することも可能である。

【００６５】

図４は、制御部１１により実行される情報蓄積処理１を示すフローチャートである。図４に示すように、制御部１１は、受信手段１５を介して医療情報ＤＢ２から医療情報を受信すると（ステップＳ１）、受信した医療情報から患者情報を抽出して（ステップＳ２）、データベース１６内において、同一の患者に関する医療情報を検索する（ステップＳ３）。そして、同一の患者に関する医療情報がデータベース１６にある場合、これらの医療情報を統合して、データベース１６に記憶させ（ステップＳ４）、本情報蓄積処理を終了する。

【００６６】

次に、図５は、制御部１１により実行される情報利用処理１を示すフローチャートである。図５に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ１１）、個人認証手段１２により、個人情報を抽出させて、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う（ステップＳ１２）。次いで、個人認証が成功した場合（ステップＳ１３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセ

ス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップＳ１４）。

【００６７】

アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ１４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧、追加、修正あるいは加工を行わせる（ステップＳ１５）。さらに、制御部１１は、端末装置Ａ～Ｅを介して、医療情報の出力指示が入力された場合（ステップＳ１６；ＹＥＳ）、出力許可手段１４により、指示された医療情報が出力可能な情報であるかを判断させる（ステップＳ１７）。そして、医療情報が出力可能な情報である場合、制御部１１は、出力許可手段１４を介して、当該医療情報を出力装置ｘ～ｚに出力させ（ステップＳ１８）、本情報利用処理を終了する。

【００６８】

以上のように、管理サーバ１ａは、医療情報ＤＢ２の自動送信手段２１から自動送信される医療情報を、患者情報に基づいて患者毎に蓄積して管理するため、医療情報管理システム１００内の医療情報を一括して管理することができ、管理サーバ１に重複した医療情報が蓄積されることがない。これにより、医療情報管理システム１００の資源を有効に利用して、効率の良い医療情報の管理を行うことができる。

【００６９】

また、この管理サーバ１ａに蓄積された医療情報を利用するためには、個人照合手段１２により、操作端末Ａ～Ｅの操作者の個人認証を行い、この個人照合手段１２により認証特定された操作者がアクセス可能な医療情報をデータアクセス権確認手段１３により確認した上で、医療情報へのアクセスを許可する。これにより、第３者は、管理サーバ１ａに記憶される医療情報に許可なくアクセスすることができない構成となり、管理サーバ１の医療情報を故意に閲覧、追加、修正あるいは加工するような不正行為を防止することができ、管理サーバ１ａに記憶される医療情報の信頼性を向上させることができる。

【００７０】

さらに、記録媒体に電子情報として記録あるいは印刷媒体にハードコピーとして出力する指示が入力された場合は、出力許可手段１４により、指示された医療情報が出力可能な情報であるかを判断して医療情報の出力が許可された場合に、出力装置ｘ～ｚに出力させる。したがって、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、プライバシーの侵害を防いで、情報管理のセキュリティを向上させることができる。

【００７１】

なお、図３では管理サーバ１に必要な情報を自動的にデータ送信する複数の医療情報ＤＢとして５個の医療ＤＢ２～６を記載したが２種以上であれば特に制限はない。また、図３では管理サーバ１を操作する操作端末Ａ～Ｅを５個備える構成にしたが、これらは必要に応じて複数用意することができ、操作端末Ａ～Ｅはネットワークｌを介して、さらにはインターネットを介して用途に応じて種々の場所に設置することができる。さらに、前述の図１あるいは図２で説明した様に医療情報ＤＢ２～８に設けられている操作端末２０～８０、医療機関ＤＢａ～ｇに設けられている操作端末ａ１～ｇ１を用いて前記管理サーバ１ａ、１ｂにアクセスして追加、変更、閲覧が可能な構成としても良い。加えて出力装置ｘ～ｚにおいても図３では３個で記載したが１個以上であれば特に制限はなく、また出力装置自体もネットワークｌを介して他の場所に設置されていても良く、操作端末Ａ～Ｅに接続する形で出力装置ｘ～ｚが接続されていても良い。なお、後述で説明する第２から第７の実施の形態においても同様である。

【００７２】

[第２の実施の形態]

次に、本発明を適用した第２の実施の形態について説明する。

図６は、本第２の実施の形態における管理サーバ１ｂの要部構成を示すブロック図である。図６に示すように、管理サーバ１ｂは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、受信手段１５、データベース１６、データ改竄防止手段１７等を備えて構成されている。すなわち、管理サーバ１ｂは、上述した第１の実施の形態における管理サーバ１ａと比較して、出力許可手段１４の代わりに、データ改竄防止手段１７を新たに備える構成となっている。なお

、データ改竄防止手段１７を除く各構成部分については、上述した第１の実施の形態における管理サーバ１ａと同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第２の実施の形態に特徴的な構成及び動作について説明する。

【００７３】

データ改竄防止手段１７は、データベース１６に記憶される医療情報に追加、修正あるいは加工する場合において、元の情報は保持したまま、元の情報への変更を履歴として記憶することにより、医療情報が改竄されることを防止する。これにより、誤って大事な医療情報を書き換えてしまう事を防止するとともに、データベース１６の医療情報を故意に追加、修正あるいは加工するような不正行為を防止でき、蓄積された医療情報のセキュリティを確保することができる。

【００７４】

次に、本第２の実施の形態における動作を説明する。管理サーバ１ｃの制御部１１は、本第２の実施の形態に特徴的な処理として情報利用処理２を実行する。図７は、制御部１１により実行される情報利用処理２を示すフローチャートである。図７に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ２１）、個人認証手段１２により、個人情報を抽出させて、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う（ステップＳ２２）。次いで、個人認証が成功した場合（ステップＳ２３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセス要求された医療情報が、アクセス可能な医療情報であるか否かを判断する（ステップＳ２４）。

【００７５】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ２４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップＳ２５）。制御部１１は、データベース１６に記憶される医療情報に追加、修正又は加工が行われた場合、データ改竄防止手段１７により、これらの変更履歴を当該医療情報に対応付けて記憶させる（ステップＳ２６）。

そして、制御部１１は、医療情報への追加、修正又は加工が終了したか否かを判別し（ステップＳ２７）、医療情報の変更が終了した場合は（ステップＳ２７；ＹＥＳ）、本情報利用処理２を終了する。また、医療情報の変更が終了していない場合（ステップＳ２７；ＮＯ）、制御部１１は、ステップＳ２５に移行して、上述した処理を繰り返して実行する。

【００７６】

以上のように、本第２の実施の形態において、管理サーバ１ｂは、データ改竄防止手段１７により、管理サーバ１ｂのデータベース１６に記憶される医療情報に追加、修正又は加工が行われた場合、元の医療情報を保持したまま、この変更履歴を当該医療情報に対応付けて記憶する。これにより、データベース１６に記憶される医療情報が書き換えられたり、不正に改竄されることを防いで、医療情報の信頼性を向上させることができる。また、元の医療情報が保持されたまま、変更履歴が記憶されるため、例えば、医療事故等が発生した場合に、不都合な記録が消去され、情報が隠蔽されてしまうことがない。

【００７７】

［第３の実施の形態］

次に、本発明を適用した第３の実施の形態について説明する。

図６は、本第２の実施の形態における管理サーバ１ｃの要部構成を示すブロック図である。図６に示すように、管理サーバ１ｃは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、受信手段１５、データベース１６、日付日時付与手段１８等を備えて構成されている。すなわち、管理サーバ１ｃは、上述した第１の実施の形態における管理サーバ１ａと比較して、出力許可手段１４の代わりに、日付日時入力手段１８を新たに備える構成となっている。なお、日付日時付与手段１８を除く各構成部分については、上述した第１の実施の形態における管理サーバ１ａと同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第３の実施の形態に特徴的な構成及び動作について説明する。

【００７８】

日付日時付与手段１８は、前記複数の医療情報ＤＢ２～６から医療情報が送信

され、受信手段１５により受信した日時を付帯情報として付与する。また、管理サーバ１ｃのデータベース１６に記憶される医療情報の閲覧、追加、修正又は加工された日時を付帯情報として付与する。なお、日付日時付与手段１８は、受信手段１５により受信された情報がデータベース１６に記憶された日時を付帯情報として付与する構成であっても良い。

【００７９】

これにより、管理サーバ１ｃに新規の医療情報が送信又は記憶された履歴や、管理サーバ１ｃのデータベース１６に記憶される医療情報が閲覧、追加、修正又は加工された履歴を過去にさかのぼって確認することができ、蓄積された医療情報の変遷を容易に把握することができる。これにより、例えば、医療情報が臨床検査管理システムデータ、放射線科情報システムデータ、病院情報システムデータ、電子カルテシステムデータ、症例管理システムデータおよび薬歴管理システムデータ等である場合、患者の状態の変化を時系列に従って観察することができ、医師による診断精度及び診断効率を向上させることができる。

【００８０】

次に、本第３の実施の形態における動作を説明する。制御部１１は、本第３の実施の形態に特徴的な処理として後述する情報蓄積処理２（図９参照）及び情報利用処理３（図１０参照）を実行する。

【００８１】

図9は、制御部１１により実行される情報蓄積処理２を示すフローチャートである。図９に示すように、制御部１１は、受信手段１５を介して医療情報ＤＢ２から医療情報を受信すると（ステップＳ３１）、日付日時付与手段１８により、受信日時を取得して、受信した医療情報に付帯情報として付与させる（ステップＳ３２）。

【００８２】

次いで、制御部１１は、受信した医療情報から患者情報を抽出して（ステップＳ３３）、データベース１６において、同一の患者に関する医療情報を検索する（ステップＳ３４）。そして、同一の患者に関する医療情報がデータベース１６にある場合、これらの医療情報を統合して、付帯情報とともにデータベース１６

に記憶させ（ステップＳ３５）、本情報蓄積処理２を終了する。

【００８３】

図１０は、制御部１１により実行される情報利用処理３を示すフローチャートである。図１０に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ４１）、個人認証手段１２により、個人情報を抽出させて（ステップＳ４２）、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う。次いで、個人認証が成功した場合（ステップＳ４３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップＳ４４）。

【００８４】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ４４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップＳ４５）。そして、制御部１１は、日付日時付与手段１８により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に対応付けてデータベース１６に記憶させ（ステップＳ４６）、本情報利用処理３を終了する。

【００８５】

以上のように、本第３の実施の形態において、管理サーバ１ｃは、日付日時付与手段１８により、データベース１６に新規な医療情報が記憶された日時や、データベース１６に記憶される医療情報の追加、修正又は加工された日時を、当該医療情報に付与する。これにより、医療情報の変遷を時系列に基づいて確認することができ、患者の状態の変化を的確に把握することができ、医師の診断精度及び診断効率を向上させることができる。また、医療情報を追加、修正又は加工した日時が限定されることにより、不正に医療情報を操作する行為を抑制する効果が得られる。

【００８６】

［第４の実施の形態］

次に、本発明を適用した第４の実施の形態について説明する。

図１１は、本第４の実施の形態における管理サーバ１ｄの要部構成を示すブロック図である。図１１に示すように、管理サーバ１ｄは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、出力許可手段１４、受信手段１５、データベース１６、データ改竄防止手段１７等を備えて構成されている。すなわち、管理サーバ１ｄは、上述した第１の実施の形態における管理サーバ１ａと比較して、データ改竄防止手段１７をさらに備える構成となっている。なお、各構成部分については、上述した第１の実施の形態における管理サーバ１ａ又は第２の実施の形態における管理サーバ１ｂと同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第４の実施の形態に特徴的な動作について説明する。

【００８７】

制御部１１は、本第４の実施の形態に特徴的な処理として、後述する情報利用処理４（図１２参照）を実行する。図１２は、制御部１１により実行される情報利用処理４を示すフローチャートである。図１２に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ５１）、個人認証手段１２により、個人情報を抽出させて、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う（ステップＳ５２）。次いで、個人認証が成功した場合（ステップＳ５３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップＳ５４）。

【００８８】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ５４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップＳ５５）。制御部１１は、データベース１６に記憶される医療情報に追加、修正又は加工が行われた場合、データ改竄防止手段１７により、これらの変更履歴を当該医療情報に対応付けて記憶させる（ステップＳ２６）。そして、制御部１１は、医療情報への追加、修正又は加工が終了したか否かを判

別し（ステップＳ５７）、これらの変更が終了した場合は（ステップＳ２７；ＹＥＳ）、操作端末Ａ～Ｅから出力指示が入力されたか否かを判別する（ステップＳ５８）。

【００８９】

端末装置Ａ～Ｅを介して、医療情報の出力指示が入力された場合（ステップＳ５８；ＹＥＳ）、制御部１１は、出力許可手段１４により指示された医療情報が出力可能な情報であるかを判断させる（ステップＳ５９）。そして、医療情報が出力可能な情報である場合、制御部１１は、出力許可手段１４を介して、当該医療情報を出力装置ｘ～ｚに出力させ（ステップＳ６０）、本情報利用処理４を終了する。

【００９０】

以上のように、本第４の実施の形態において、管理サーバ１ｄは、データ改竄防止手段１７により、管理サーバ１ｄのデータベース１６に記憶される医療情報に追加、修正又は加工が行われた場合、元の医療情報を保持したまま、この変更履歴を当該医療情報に対応付けて記憶する。また、出力許可手段１４により、出力指示された医療情報が出力可能な情報であるかを判断し、医療情報の出力が許可された場合に、医療情報を出力させる。これにより、管理サーバ１の医療情報を故意に閲覧、追加、修正あるいは加工するような不正行為を防止するとともに、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、情報管理のセキュリティを向上させることができる。

【００９１】

[第５の実施の形態]

次に、本発明を適用した第５の実施の形態について説明する。

図１３は、本第５の実施の形態における管理サーバ１ｅの要部構成を示すブロック図である。図１３に示すように、管理サーバ１ｅは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、出力許可手段１４、受信手段１５、データベース１６、日付日時付与手段１８等を備えて構成されている。すなわち、管理サーバ１ｅは、上述した第１の実施の形態における管理サーバ１ａと比較して、日付日時付与手段１８をさらに備える構成となっている。なお、各構成部

分については、上述した第１の実施の形態における管理サーバ１ａ又は第３の実施の形態における管理サーバ１ｃと同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第５の実施の形態に特徴的な動作について説明する。

【００９２】

制御部１１は、本第５の実施の形態に特徴的な処理として、情報蓄積処理２（図９参照）及び後述する情報利用処理５（図１４参照）を実行する。なお、情報蓄積処理２については、上述した第３の実施の形態における情報蓄積処理２と同一の処理であるため、説明を省略する。

【００９３】

図１４は、制御部１１により実行される情報利用処理５を示すフローチャートである。図１４に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ６１）、個人認証手段１２により、個人情報を抽出させて（ステップＳ６２）、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う。次いで、個人認証が成功した場合（ステップＳ６３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップＳ６４）。

【００９４】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ６４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップＳ６５）。そして、制御部１１は、日付日時付与手段１８により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に付与させる（ステップＳ６６）。

【００９５】

次いで、制御部１１は、操作端末Ａ～Ｅから出力指示が入力されたか否かを判別し（ステップＳ６７）、医療情報の出力指示が入力された場合（ステップＳ６７；ＹＥＳ）、出力許可手段１４により、指示された医療情報が出力可能な情報

であるかを判断させる（ステップＳ６８）。そして、医療情報が出力可能な情報である場合（ステップＳ６８；ＹＥＳ）、制御部１１は、出力許可手段１４を介して、当該医療情報を出力装置ｘ～ｚに出力させ（ステップＳ６９）、本情報利用処理５を終了する。

【００９６】

以上のように、本第５の実施の形態において、管理サーバ１ｅは、日付日時付与手段１８により、データベース１６に新規な医療情報が記憶された日時や、データベース１６に記憶される医療情報の追加、修正又は加工された日時を、当該医療情報に対応付けて記憶させる。また、出力許可手段１４により、出力指示された医療情報が出力可能な情報であるかを判断し、医療情報の出力が許可された場合に、医療情報を出力させる。

【００９７】

これにより、医療情報の変遷を時系列に基づいて確認することができ、患者の状態の変化を的確に把握することができ、医師の診断精度及び診断効率を向上させることができる。また、医療情報を追加、修正又は加工した日時が限定されることにより、データベース１６の医療情報を過去にさかのぼって不正に操作する行為を抑制する効果が得られる。さらに、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、情報管理のセキュリティを向上させることができる。

【００９８】

[第６の実施の形態]

次に、本発明を適用した第６の実施の形態について説明する。

図１５は、本第６の実施の形態における管理サーバ１ｆの要部構成を示すブロック図である。図１５に示すように、管理サーバ１ｆは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、受信手段１５、データベース１６、データ改竄防止手段１７、日付日時付与手段１８等を備えて構成されている。すなわち、管理サーバ１ｆは、上述した第１の実施の形態における管理サーバ１ａと比較して、出力許可手段１４の代わりに、データ改竄防止手段１７及び日付日時付与手段１８をさらに備える構成となっている。なお、各構成部分については

、上述した第１の実施の形態における管理サーバ１ａ、第２の実施の形態における管理サーバ１ｂ、第３の実施の形態における管理サーバ１ｃと同一の構成によってなるため、同一の構成部分については詳細な説明を省略する。以下では、本第６の実施の形態に特徴的な動作について説明する。

【００９９】

制御部１１は、本第６の実施の形態に特徴的な処理として、情報蓄積処理２（図９参照）及び後述する情報利用処理６（図１６参照）を実行する。なお、情報蓄積処理２については、上述した第３の実施の形態における情報蓄積処理２と同一の処理であるため、説明を省略する。

【０１００】

図１６は、制御部１１により実行される情報利用処理６を示すフローチャートである。図１６に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ７１）、個人認証手段１２により、個人情報を抽出させて（ステップＳ７２）、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う。次いで、個人認証が成功した場合（ステップＳ７３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップＳ７４）。

【０１０１】

次いで、アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ７４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップＳ７５）。制御部１１は、日付日時付与手段１８により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に付与させる（ステップＳ７６）。さらに、データ改竄防止手段１７により、これらの変更履歴を当該医療情報に対応付けてデータベース１６に記憶させる（ステップＳ７７）。

【０１０２】

そして、制御部１１は、医療情報への追加、修正又は加工が終了したか否かを

判別し（ステップＳ７８）、医療情報の変更が終了した場合は（ステップＳ７８；ＹＥＳ）、本情報利用処理６を終了する。また、医療情報の変更が終了していない場合（ステップＳ７８；ＮＯ）、制御部１１は、ステップＳ７５に移行して、上述した処理を繰り返して実行する。

【０１０３】

以上のように、本第６の実施の形態によれば、管理サーバ１ｅは、日付日時付与手段１８により、データベース１６に新規な医療情報が記憶された日時を付帯情報として当該医療情報に付与する。また、データ改竄防止手段１７及び日付日時付与手段１８により、データベース１６に記憶される医療情報が追加、修正又は加工された場合、その変更履歴及び変更日時を当該医療情報に対応付けて記憶する。

【０１０４】

これにより、医療情報の変遷を時系列に基づいて確認することができ、患者の状態の変化を的確に把握することができ、医師の診断精度及び診断効率を向上させることができる。また、医療情報を追加、修正又は加工した日時及び変更履歴が限定されることにより、データベース１６の医療情報を過去にさかのぼって不正に改竄されることを防いで、医療情報の信頼性を向上させることができる。

【０１０５】

［第７の実施の形態］

次に、本発明を適用した第７の実施の形態について説明する。

図１７は、本第６の実施の形態における管理サーバ１ｇの要部構成を示すブロック図である。図１７に示すように、管理サーバ１ｆは、制御部１１、個人照合手段１２、データアクセス権確認手段１３、出力許可手段１４、受信手段１５、データベース１６、データ改竄防止手段１７、日付日時付与手段１８等を備えて構成されている。すなわち、管理サーバ１ｆは、上述した第１の実施の形態における管理サーバ１ａと比較して、データ改竄防止手段１７及び日付日時付与手段１８をさらに備える構成となっている。なお、各構成部分については、上述した第１の実施の形態における管理サーバ１ａ、第２の実施の形態における管理サーバ１ｂ、第３の実施の形態における管理サーバ１ｃと略同一の構成によってなる

ため、同一の構成部分については詳細な説明を省略する。以下では、本第７の実施の形態に特徴的な動作について説明する。

【０１０６】

制御部１１は、本第７の実施の形態に特徴的な処理として、情報蓄積処理２（図９参照）及び後述する情報利用処理７（図１８参照）を実行する。なお、情報蓄積処理２については、上述した第３の実施の形態における情報蓄積処理２と同一の処理であるため、説明を省略する。

【０１０７】

図１８は、制御部１１により実行される情報利用処理７を示すフローチャートである。図１８に示すように、制御部１１は、個人認証手段１２を介してアクセス要求を受信すると（ステップＳ８１）、個人認証手段１２により、個人情報を抽出させて（ステップＳ８２）、アクセス要求を送信してきた端末Ａ～Ｅを操作する操作者の個人認証を行う。個人認証が成功した場合（ステップＳ８３；ＹＥＳ）、制御部１１は、データアクセス権確認手段１３により、アクセス要求された医療情報が、アクセス可能な情報であるか否かを判断する（ステップＳ８４）。

【０１０８】

アクセス要求された医療情報がアクセス可能な情報である場合（ステップＳ８４；ＹＥＳ）、制御部１１は、アクセス要求にしたがって、データベース１６に記憶される医療情報の閲覧や、医療情報に対する追加、修正又は加工を行わせる（ステップＳ８５）。次いで、制御部１１は、日付日時付与手段１８により、医療情報の閲覧、追加、修正又は加工が行われた日時を取得し、付帯情報として当該医療情報に付与させる（ステップＳ８６）。また、制御部１１は、データ改竄防止手段１７により、これらの変更履歴を当該医療情報に対応付けて記憶させる（ステップＳ８７）。

【０１０９】

さらに、制御部１１は、医療情報への追加、修正又は加工が終了したか否かを判別し（ステップＳ８８）、医療情報の変更が終了した場合（ステップＳ８８；ＹＥＳ）、操作端末Ａ～Ｅから出力指示が入力されたか否かを判別する（ステッ

プＳ８９）。操作端末Ａ～Ｅから出力指示が入力された場合（ステップＳ８９；ＹＥＳ）、制御部１１は、出力許可手段１４により、指示された医療情報が出力可能な情報であるかを判断させる（ステップＳ９０）。そして、医療情報が出力可能な情報である場合（ステップＳ９０；ＹＥＳ）、制御部１１は、出力許可手段１４を介して、当該医療情報を出力装置ｘ～ｚに出力させ（ステップＳ９１）、本情報利用処理７を終了する。

【０１１０】

以上のように、本第７の実施の形態において、サーバ１ｇは、日付日時付与手段１８により、データベース１６に新規な医療情報が記憶された日時を付帯情報として当該医療情報に付与させる。また、データ改竄防止手段１７及び日付日時付与手段１８により、データベース１６に記憶される医療情報が追加、修正又は加工された場合、その変更履歴及び変更日時を当該医療情報に対応付けて記憶する。さらに、サーバ１ｇは、出力許可手段１４により、出力指示された医療情報が出力可能な情報であるかを判断し、医療情報の出力が許可された場合に、医療情報を出力させる。

【０１１１】

これにより、管理サーバ１ｇのデータベース１６に記憶される医療情報を過去にさかのぼって、閲覧、追加、修正あるいは加工するような不正行為を防止するとともに、患者の個人情報の外部への流失や医療情報の別の記録媒体へのコピーを防止することができ、情報管理のセキュリティを向上させることができる。また、医療情報が新規に送信又は記憶された日時や、医療情報の更新された日時を記憶するため、医療情報の変遷が明確になり、患者の状態の変化を容易に確認できる。これにより、医師の診断効率、診断制度を向上させることができる。

【０１１２】

なお、上述した第１から第７の実施の形態における記述は、本発明に係る医療情報管理システムの一例であり、これらに限定されるものではない。

【０１１３】

例えば、管理サーバ１ａ～１ｇに備えるデータベース１６は、単一のハードディスクで形成されるか、単一のハードディスクに複数のボリュームあるいはパー

ティションを切ったものでも良く、さらには複数のハードディスクを並列に繋げたもの、複数に繋げた個々のハードディスクに複数のボリュームあるいはパーティションを切ったものでも良い。なお、必要な情報を短時間で送受信したり、ハードディスクがクラッシュした際の復旧の容易性あるいはバックアップの容易性の問題から、図１９に示すように、データベース１６に複数のデータベースＡ～Ｅを備えて構成されるものが好ましい。この場合、制御部１１は、操作端末Ａ～Ｅから送信されるアクセス要求に応じて、データベースＡ～Ｅから必要な医療情報を選択して取得する。

【０１１４】

また、例えば、医療情報管理システム２００において、管理サーバ１、医療機関ＤＢａ～ｇ、操作端末ａ１～ｇ１、操作端末α～εを接続するネットワークは、それぞれ専用回線により構築されることがセキュリティ上好ましいが、例えば、地域の中核となる病院とかかりつけ医などの小規模病院間の接続のように、専用回線で接続することが難しい場合においては、送受信する情報を暗号化することが情報の漏洩を防ぐ意味から好ましい。この場合、管理サーバ１、医療機関ＤＢａ～ｇ、操作端末ａ１～ｇ１、操作端末α～εに暗号化手段（図示せず）及び復号化手段（図示せず）を備え、例えば、秘密鍵暗号、公開鍵暗号等を用いて送受信する情報の暗号化及び復号化を行う。また、暗号化される情報は、医療情報に限らず、上述したアクセス要求に含まれる操作指示や操作者の個人情報等を含むことが好ましい。

【０１１５】

その他、本第１から第７の実施の形態における医療情報管理システムにおける構成部分の細部構成、及び細部動作に関しては、本発明の趣旨を逸脱することのない範囲で適宜変更可能であることはもちろんである。

【０１１６】

【発明の効果】

本発明によれば、統合的に医療情報が管理される医療情報管理システムにおいて、医療情報を操作する操作者の認証を行うともに、認証された操作者により操作される医療情報が、操作可能な情報であるかを確認することにより、医療情報

が不正に操作されることを防いで、情報管理のセキュリティを向上させることができる。また、医療情報を出力する際は、出力指示された医療情報が出力可能な情報であるかを確認した後に出力するため、重要な医療情報が外部に漏洩することを防止することができる。

【０１１７】

さらに、医療情報に追加、修正あるいは加工等の操作が行われた場合は、元の医療情報を保持したまま、当該医療情報に対応付けて変更履歴を記憶するため、重要な医療情報が誤って書き換えられたり、不正に医療情報が改竄されることを防止できる。また、医療情報の記憶日時や変更された日時を付帯情報として医療情報に付与するため、これらの日時が限定されることにより、不正に情報を操作する行為を抑制する効果が得られる。

【図面の簡単な説明】

【図１】

本発明を適用した医療情報管理システム１００のシステム構成を示す概念図である。

【図２】

本発明を適用した医療情報管理システム２００のシステム構成を示す概念図である。

【図３】

本発明を適用した第１の実施の形態における管理サーバ１ａの要部構成を示すブロック図である。

【図４】

図３に示す制御部１１により実行される情報蓄積処理１を示すフローチャートである。

【図５】

図３に示す制御部１１により実行される情報利用処理１を示すフローチャートである。

【図６】

本発明を適用した第２の実施の形態における管理サーバ１ｂの要部構成を示す

ブロック図である。

【図７】

図６に示す制御部１１により実行される情報利用処理２を示すフローチャートである。

【図８】

本発明を適用した第３の実施の形態における管理サーバ１ｃの要部構成を示すブロック図である。

【図９】

図８に示す制御部１１により実行される情報蓄積処理２を示すフローチャートである。

【図１０】

図８に示す制御部１１により実行される情報利用処理３を示すフローチャートである。

【図１１】

本発明を適用した第４の実施の形態における管理サーバ１ｄの要部構成を示すブロック図である。

【図１２】

図１１に示す制御部１１により実行される情報利用処理４を示すフローチャートである。

【図１３】

本発明を適用した第５の実施の形態における管理サーバ１ｅの要部構成を示すブロック図である。

【図１４】

図１３に示す制御部１１により実行される情報利用処理５を示すフローチャートである。

【図１５】

本発明を適用した第６の実施の形態における管理サーバ１ｆの要部構成を示すブロック図である。

【図１６】

図１５に示す制御部１１により実行される情報利用処理６を示すフローチャートである。

【図１７】

本発明を適用した第７の実施の形態における管理サーバ１ｇの要部構成を示すブロック図である。

【図１８】

図１７に示す制御部１１により実行される情報利用処理７を示すフローチャートである。

【図１９】

管理サーバ１のデータベース１６のデータ構成の一例を示す図である。

【符号の説明】

１００～２００　医療情報管理システム

１ａ～１ｇ、２　医療情報統括管理サーバ

１１　制御部

１２　個人照合手段

１３　データアクセス権確認手段

１４　出力許可手段

１５　受信手段

１６　データベース

１７　データ改竄防止手段

１８　日付日時付与手段

２～８　医療情報データベース

２１～６１　自動送信手段

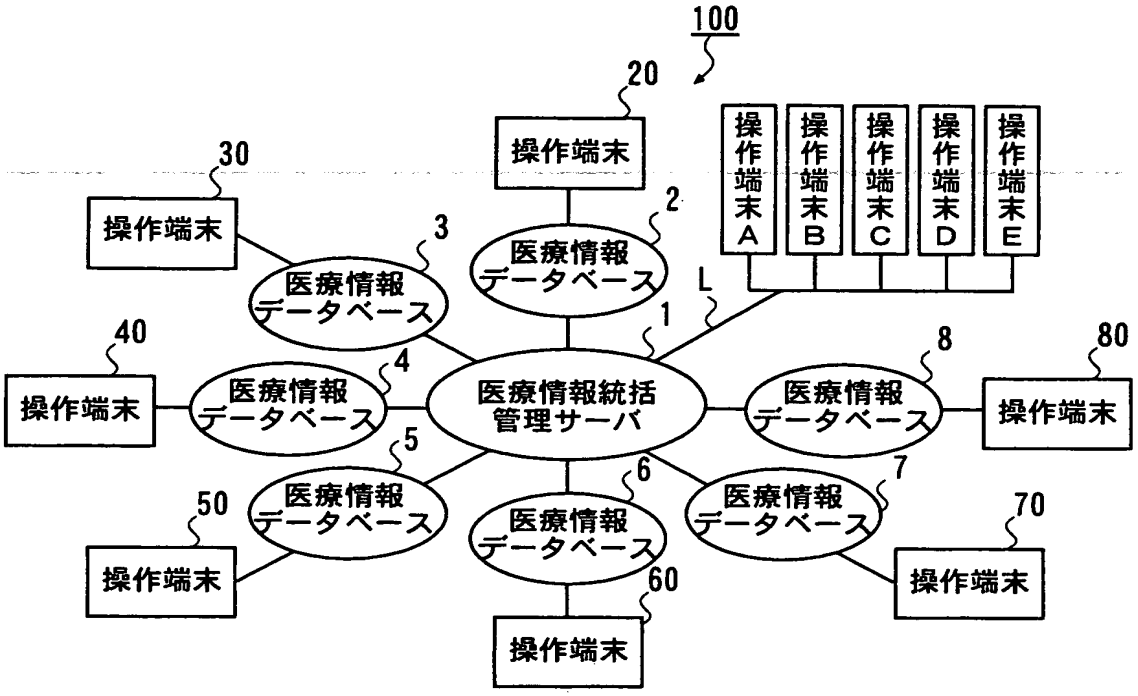
ａ～ｇ　医療機関データベース

Ａ～Ｅ、α～ε　操作端末

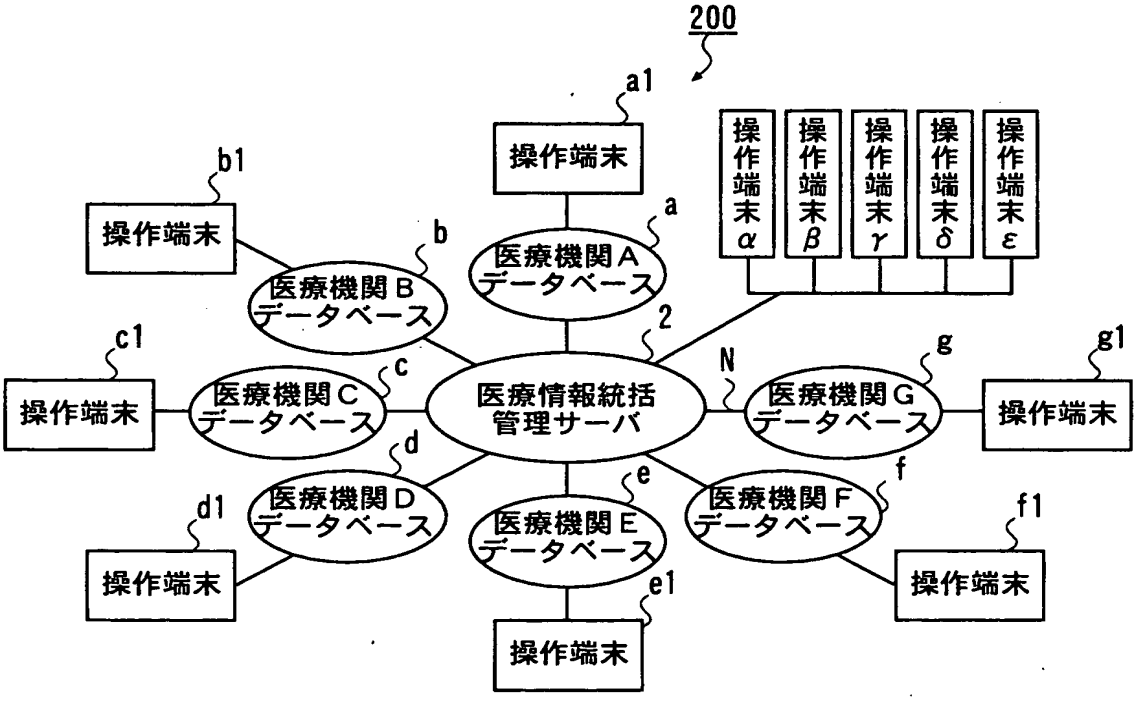
Ｌ，Ｎ　ネットワーク

【書類名】　図面

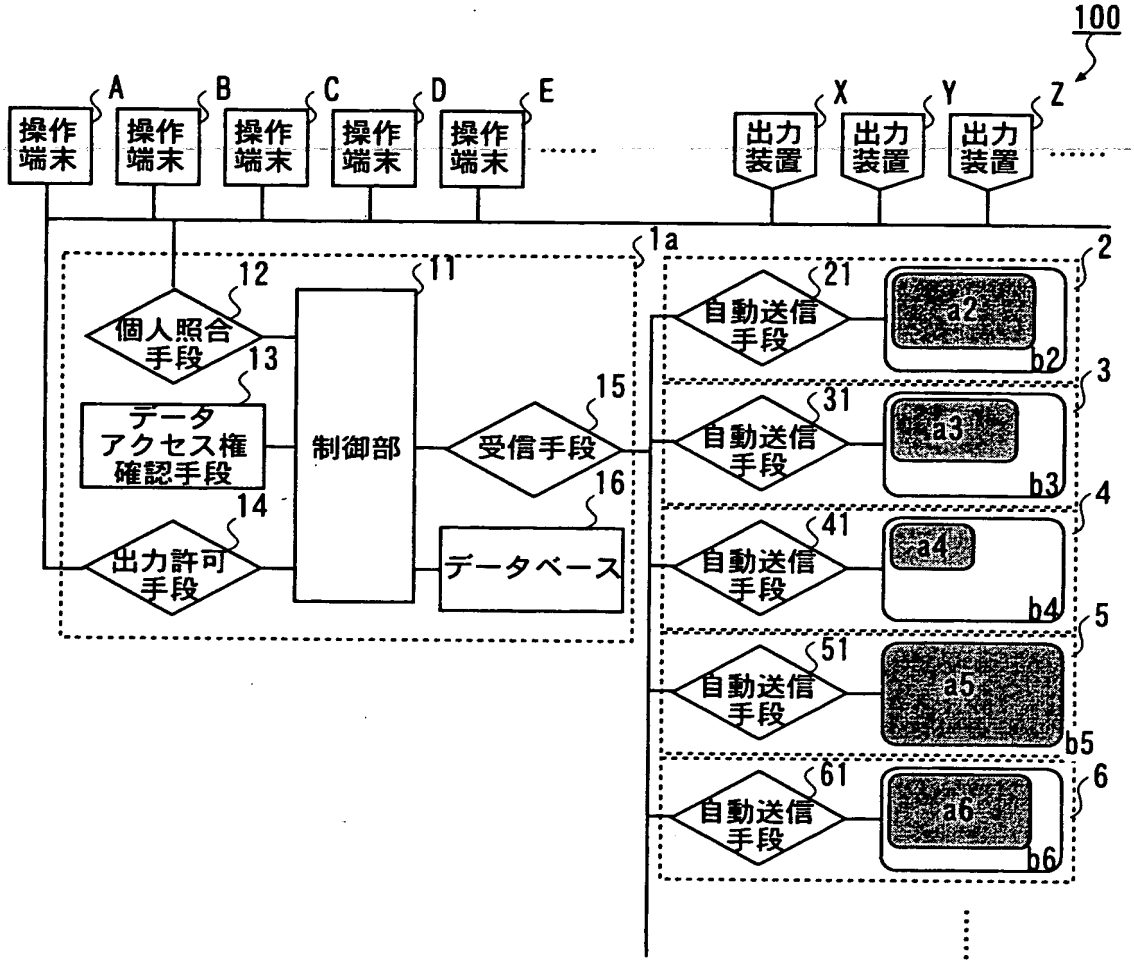
【図１】


100
20
操作端末
操作端末A
操作端末B
操作端末C
操作端末D
操作端末E
30
操作端末
2
医療情報データベース
3
医療情報データベース
L
1
40
操作端末
医療情報データベース
4
医療情報統括管理サーバ
8
医療情報データベース
80
操作端末
5
医療情報データベース
6
医療情報データベース
7
医療情報データベース
50
操作端末
70
操作端末
60
操作端末

【図２】

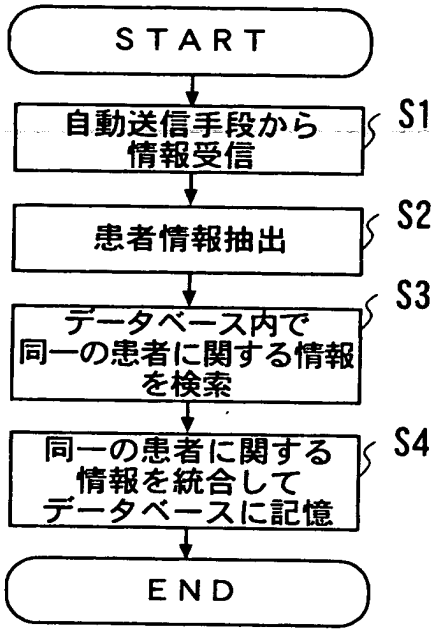

200
a1
操作端末
操作端末α
操作端末β
操作端末γ
操作端末δ
操作端末ε
b1
操作端末
a
医療機関Aデータベース
b
医療機関Bデータベース
2
c1
操作端末
c
医療機関Cデータベース
医療情報統括管理サーバ
N
g
医療機関Gデータベース
g1
操作端末
d
医療機関Dデータベース
e
医療機関Eデータベース
f
医療機関Fデータベース
d1
操作端末
f1
操作端末
e1
操作端末

【図３】

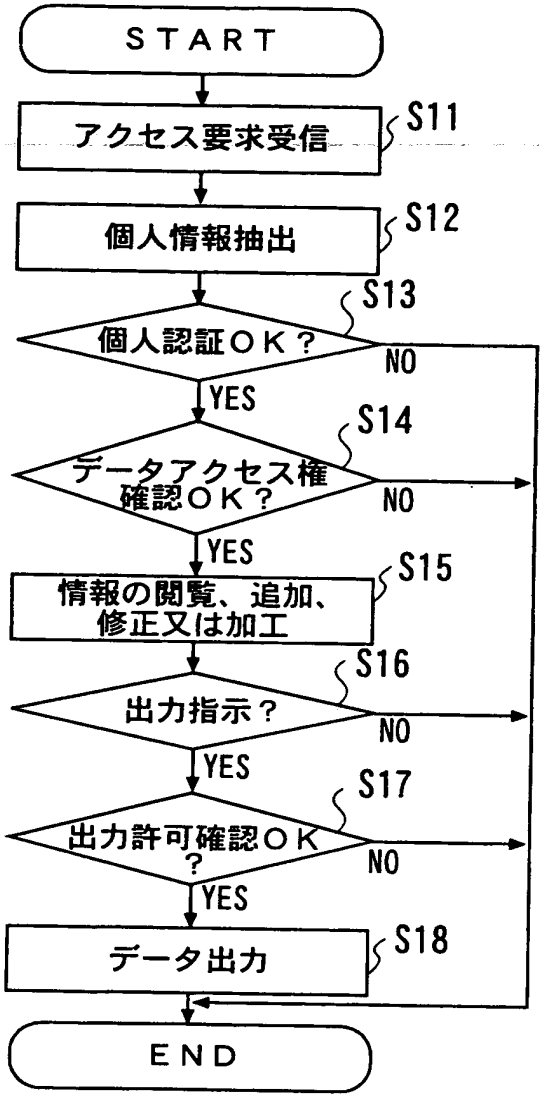


出証特２００３－３０４５３３０

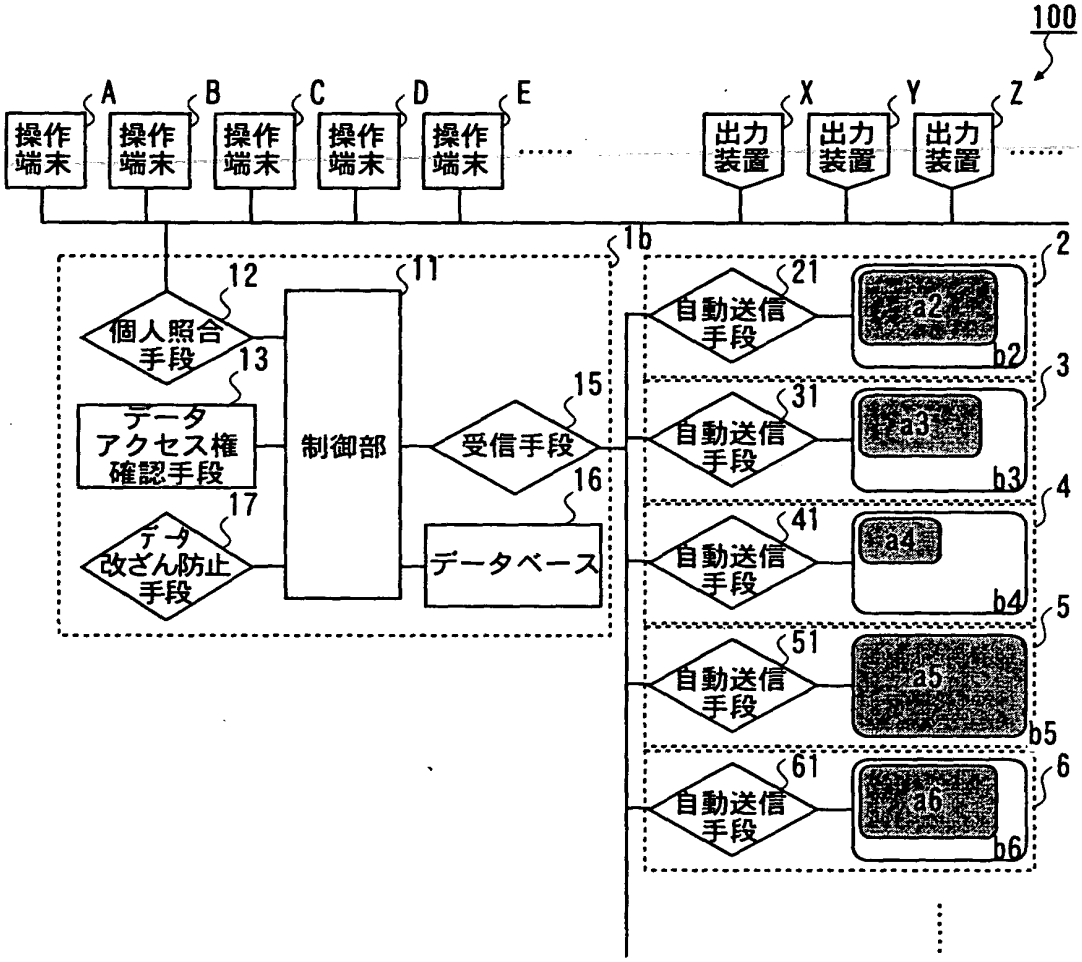
【図４】


START
自動送信手段から情報受信
S1
患者情報抽出
S2
データベース内で同一の患者に関する情報を検索
S3
同一の患者に関する情報を統合してデータベースに記憶
S4
END

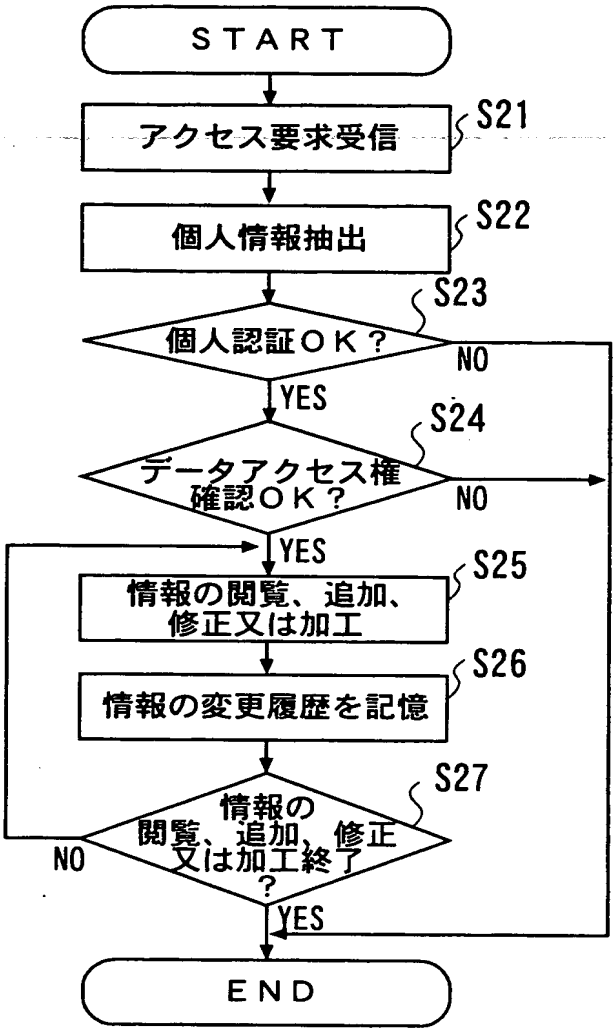
【図５】


START
アクセス要求受信
S11
個人情報抽出
S12
個人認証ＯＫ？
S13
NO
YES
データアクセス権確認ＯＫ？
S14
NO
YES
情報の閲覧、追加、修正又は加工
S15
出力指示？
S16
NO
YES
出力許可確認ＯＫ？
S17
NO
YES
データ出力
S18
END

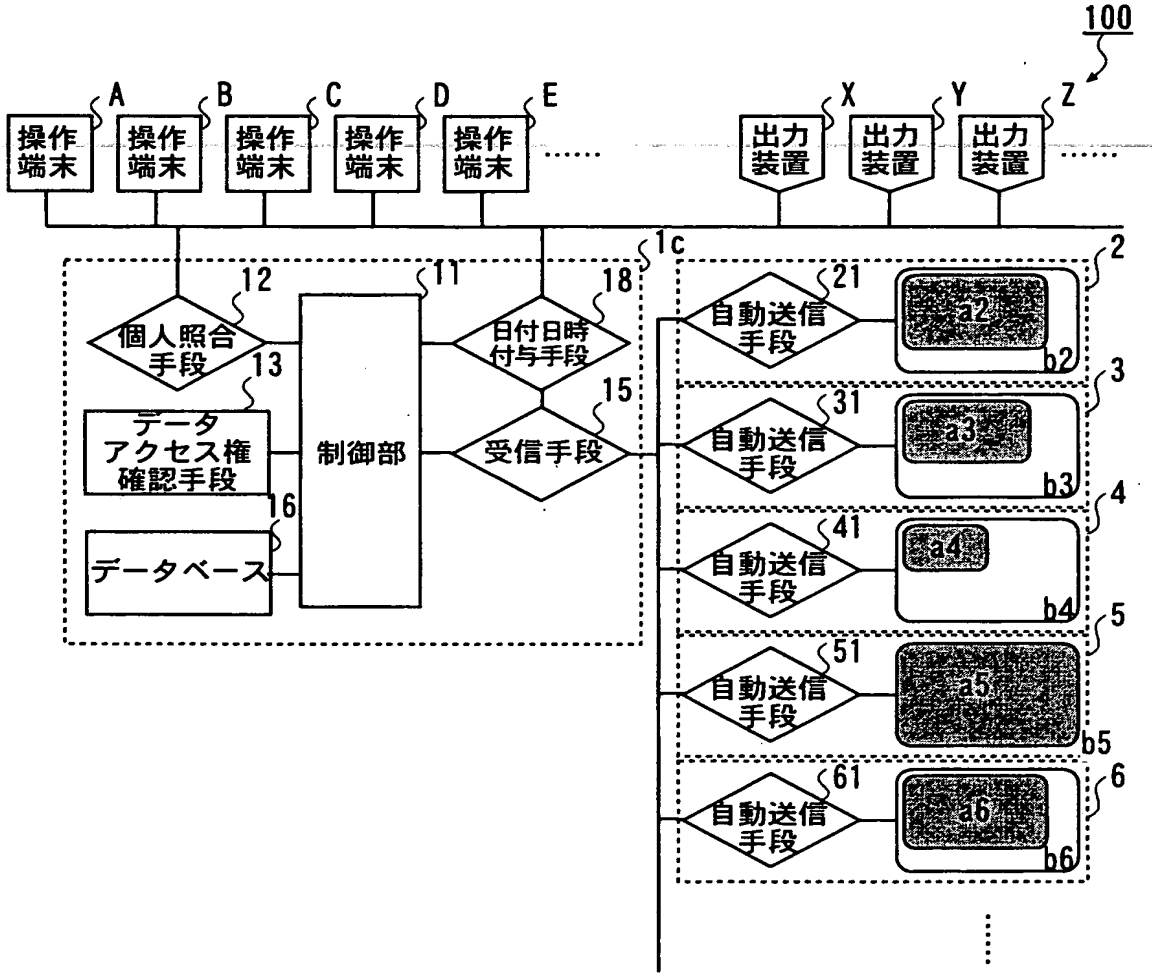
【図６】


100
A
B
C
D
E
X
Y
Z
操作端末
操作端末
操作端末
操作端末
操作端末
出力装置
出力装置
出力装置
1b
2
3
4
5
6
11
12
13
15
16
17
21
31
41
51
61
個人照合手段
データアクセス権確認手段
データ改ざん防止手段
制御部
受信手段
データベース
自動送信手段
自動送信手段
自動送信手段
自動送信手段
自動送信手段
a2
a3
a4
a5
a6
b2
b3
b4
b5
b6

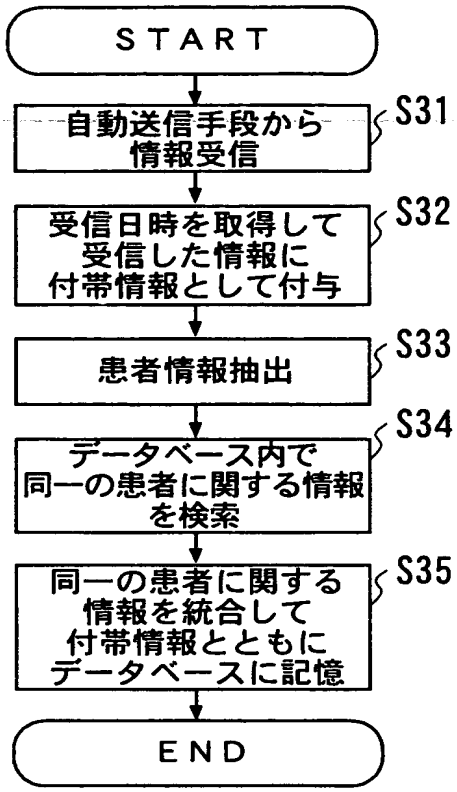
【図７】


START
アクセス要求受信
S21
個人情報抽出
S22
個人認証ＯＫ？
S23
NO
YES
データアクセス権確認ＯＫ？
S24
NO
YES
情報の閲覧、追加、修正又は加工
S25
情報の変更履歴を記憶
S26
情報の閲覧、追加、修正又は加工終了？
S27
NO
YES
END

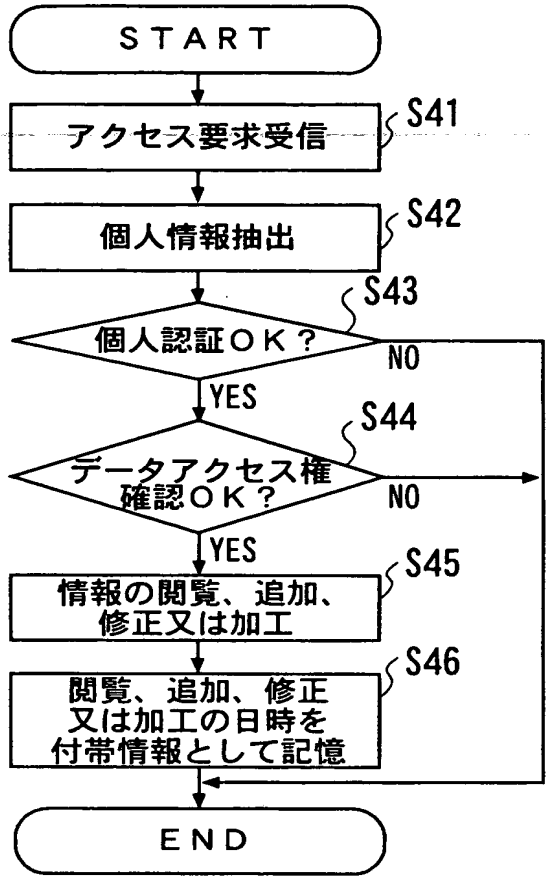
【図８】


100
A
B
C
D
E
X
Y
Z
操作端末
操作端末
操作端末
操作端末
操作端末
出力装置
出力装置
出力装置
1c
12
個人照合手段
13
データアクセス権確認手段
16
データベース
11
制御部
18
日付日時付与手段
15
受信手段
2
21
自動送信手段
a2
b2
3
31
自動送信手段
a3
b3
4
41
自動送信手段
a4
b4
5
51
自動送信手段
a5
b5
6
61
自動送信手段
a6
b6

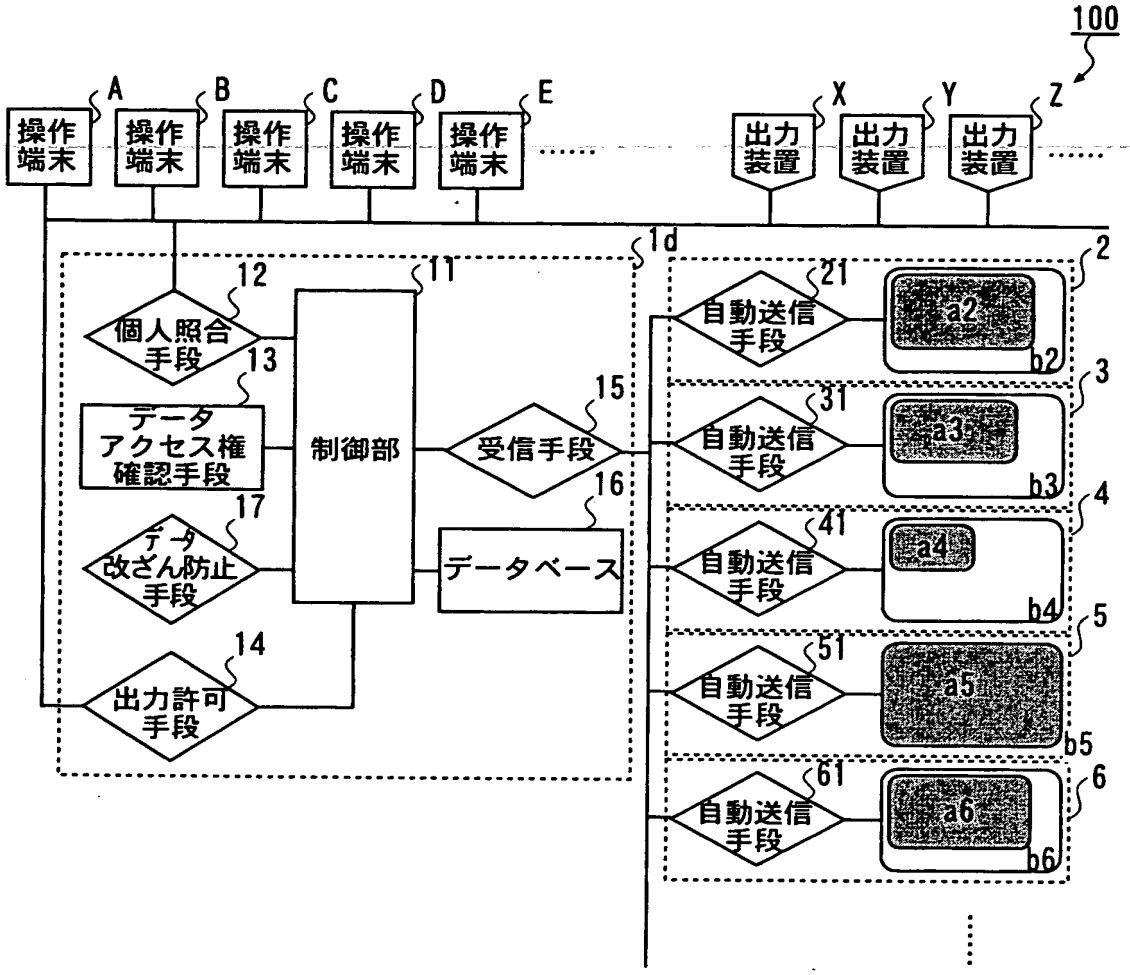
【図９】


START
自動送信手段から情報受信
S31
受信日時を取得して受信した情報に付帯情報として付与
S32
患者情報抽出
S33
データベース内で同一の患者に関する情報を検索
S34
同一の患者に関する情報を統合して付帯情報とともにデータベースに記憶
S35
END

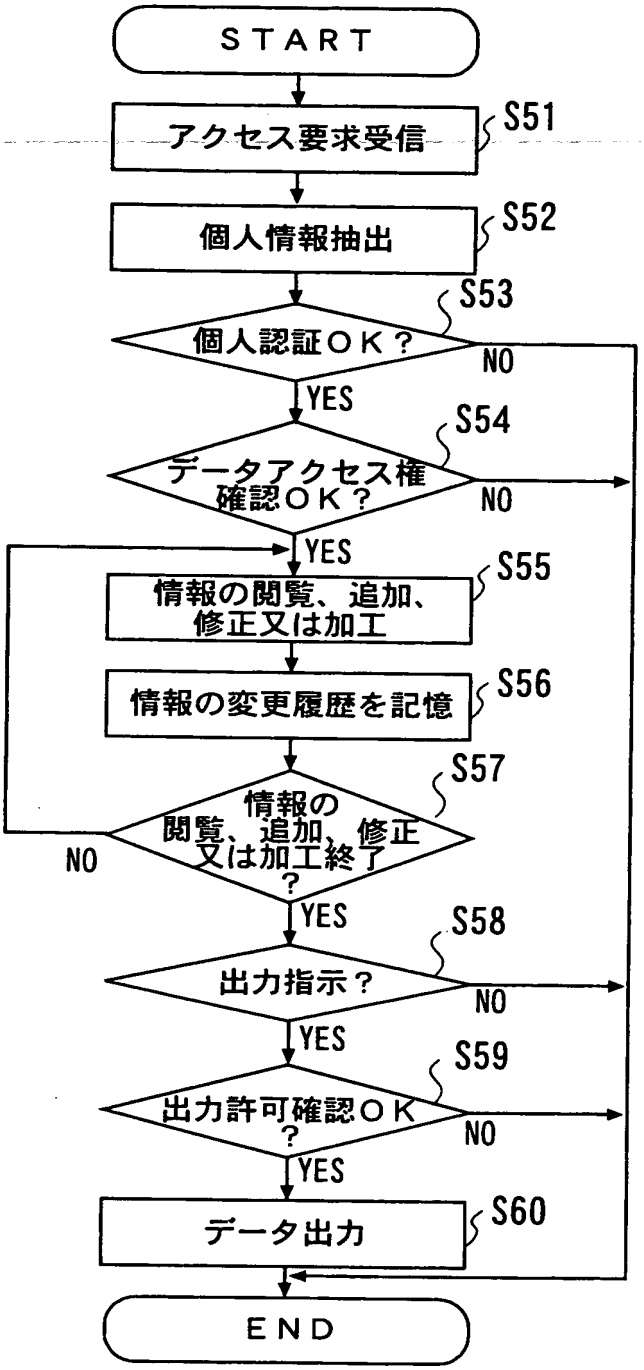
【図１０】


START
アクセス要求受信
S41
個人情報抽出
S42
S43
個人認証ＯＫ？
NO
YES
S44
データアクセス権
確認ＯＫ？
NO
YES
情報の閲覧、追加、
修正又は加工
S45
閲覧、追加、修正
又は加工の日時を
付帯情報として記憶
S46
END

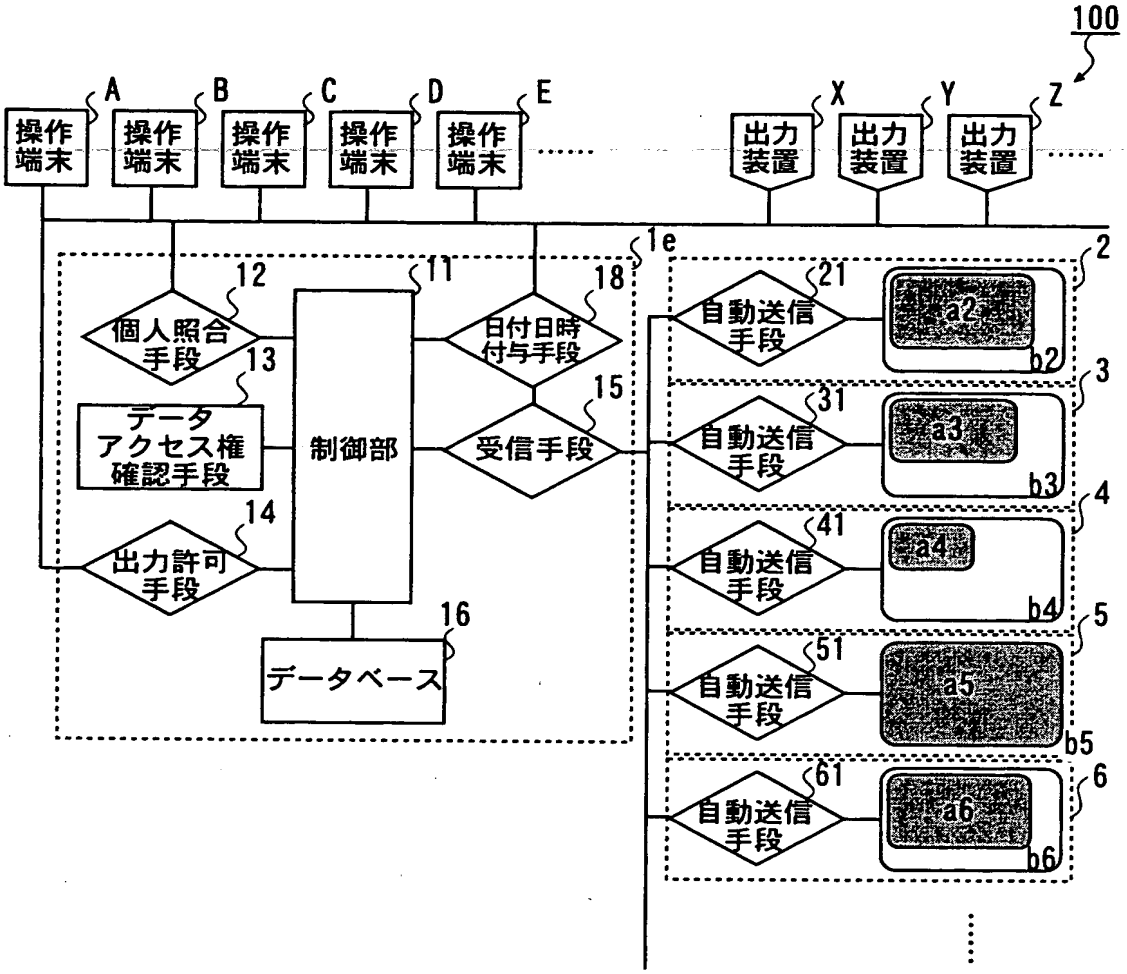
【図１１】


100
A
B
C
D
E
X
Y
Z
操作端末
操作端末
操作端末
操作端末
操作端末
出力装置
出力装置
出力装置
1d
2
3
4
5
6
11
12
13
14
15
16
17
個人照合手段
データアクセス権確認手段
データ改ざん防止手段
出力許可手段
制御部
受信手段
データベース
21
31
41
51
61
自動送信手段
自動送信手段
自動送信手段
自動送信手段
自動送信手段
a2
a3
a4
a5
a6
b2
b3
b4
b5
b6

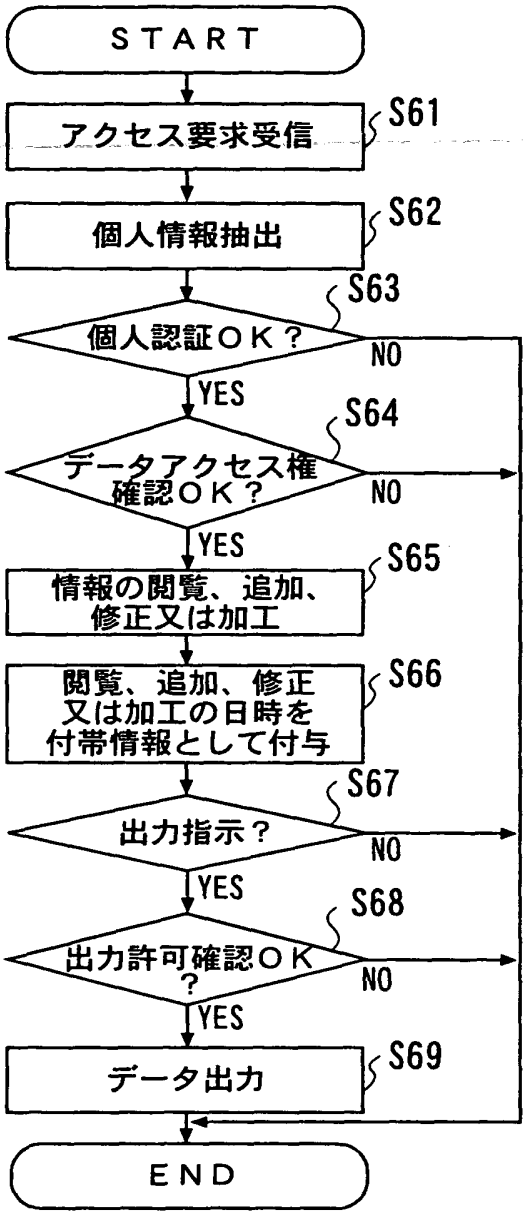
【図１２】


START
アクセス要求受信
S51
個人情報抽出
S52
個人認証ＯＫ？
S53
NO
YES
データアクセス権確認ＯＫ？
S54
NO
YES
情報の閲覧、追加、修正又は加工
S55
情報の変更履歴を記憶
S56
情報の閲覧、追加、修正又は加工終了？
S57
NO
YES
出力指示？
S58
NO
YES
出力許可確認ＯＫ？
S59
NO
YES
データ出力
S60
END

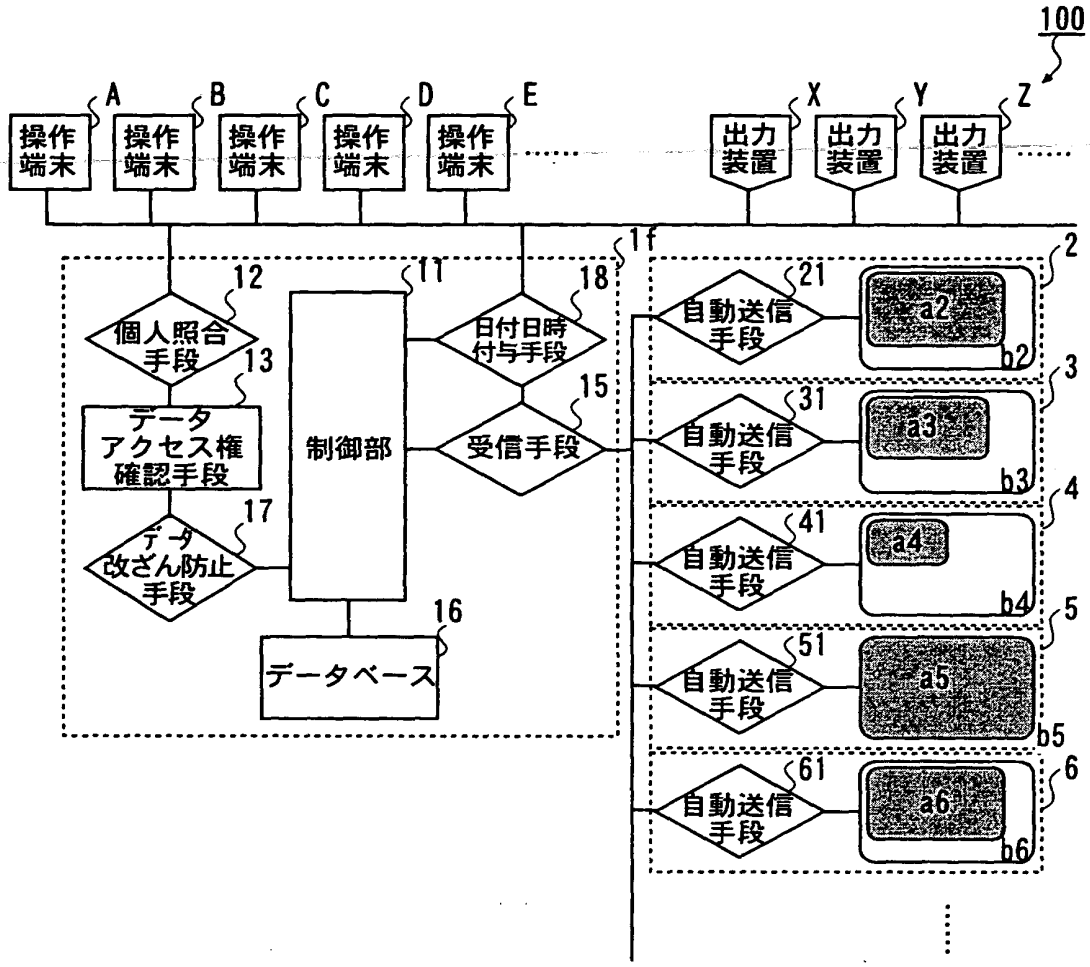
【図１３】


100
A
B
C
D
E
X
Y
Z
操作端末
操作端末
操作端末
操作端末
操作端末
出力装置
出力装置
出力装置
1e
2
3
4
5
6
11
12
13
14
15
16
18
個人照合手段
データアクセス権確認手段
出力許可手段
制御部
データベース
日付日時付与手段
受信手段
21
31
41
51
61
自動送信手段
自動送信手段
自動送信手段
自動送信手段
自動送信手段
a2
a3
a4
a5
a6
b2
b3
b4
b5
b6

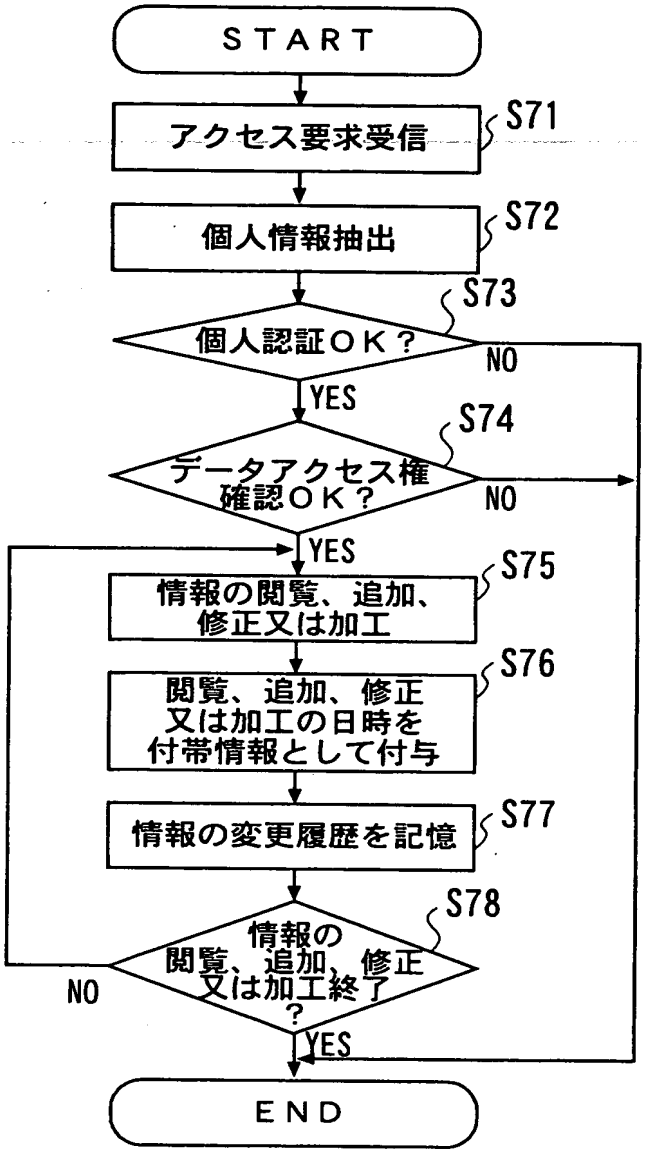
【図１４】


START
アクセス要求受信
S61
個人情報抽出
S62
個人認証ＯＫ？
S63
NO
YES
データアクセス権確認ＯＫ？
S64
NO
YES
情報の閲覧、追加、修正又は加工
S65
閲覧、追加、修正又は加工の日時を付帯情報として付与
S66
出力指示？
S67
NO
YES
出力許可確認ＯＫ？
S68
NO
YES
データ出力
S69
END

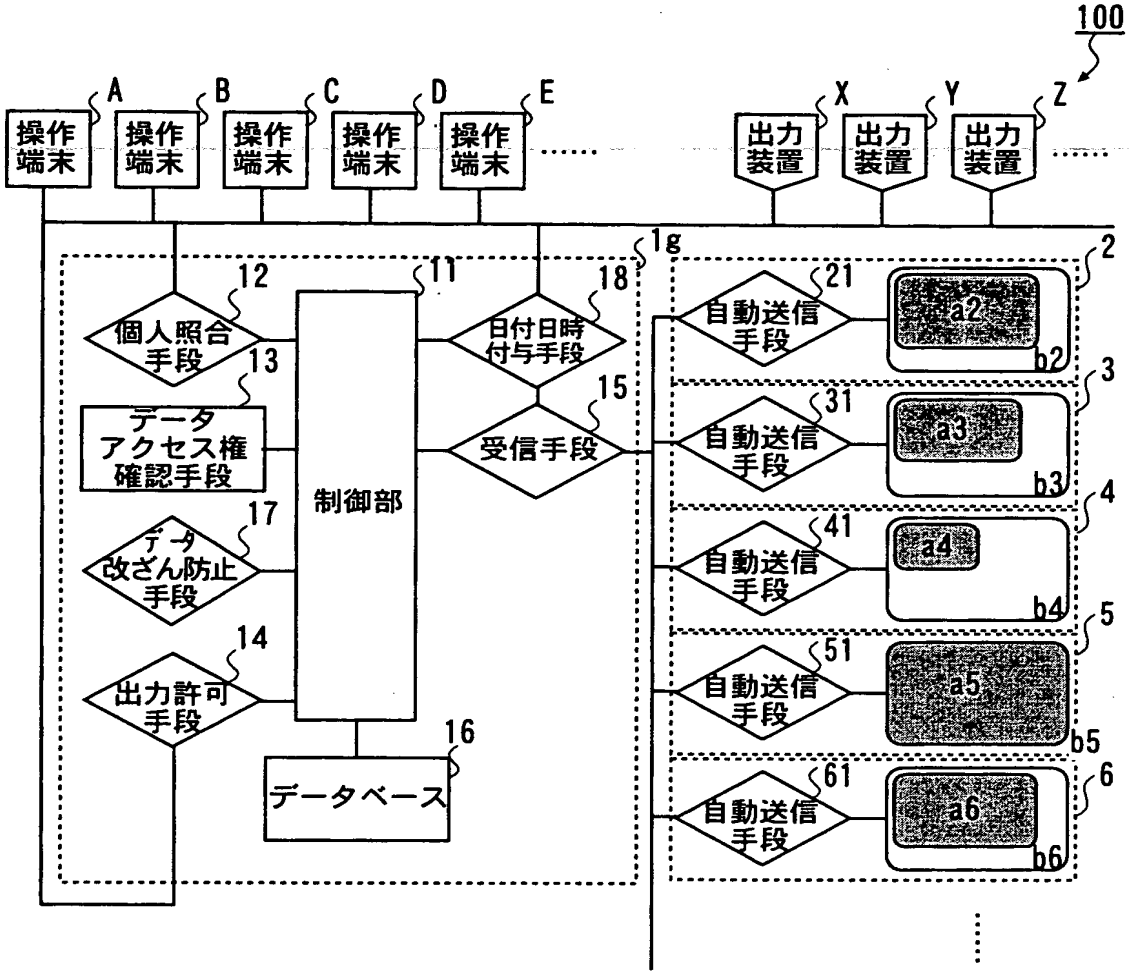
【図１５】


100
A
B
C
D
E
X
Y
Z
操作端末
操作端末
操作端末
操作端末
操作端末
出力装置
出力装置
出力装置
1f
12
個人照合手段
13
データアクセス権確認手段
17
データ改ざん防止手段
11
制御部
16
データベース
18
日付日時付与手段
15
受信手段
2
21
自動送信手段
a2
b2
3
31
自動送信手段
a3
b3
4
41
自動送信手段
a4
b4
5
51
自動送信手段
a5
b5
6
61
自動送信手段
a6
b6

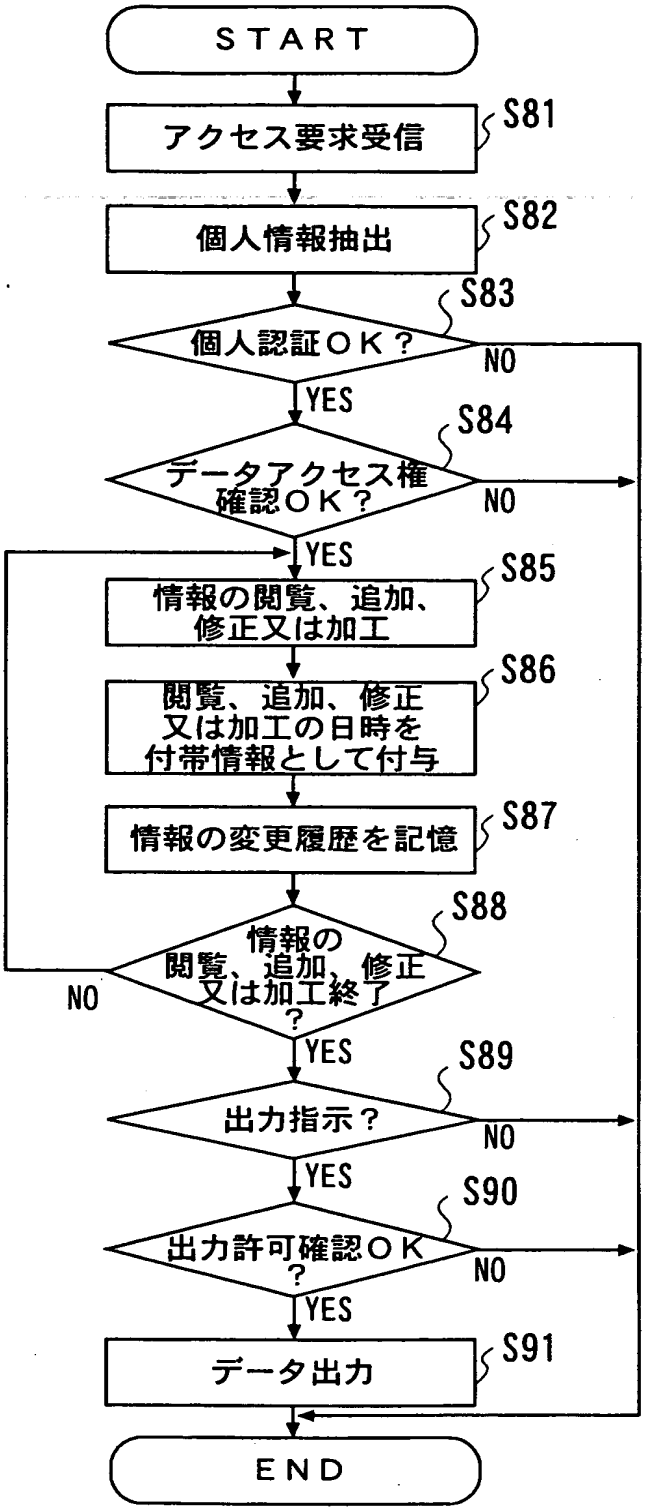
【図１６】


START
アクセス要求受信
S71
個人情報抽出
S72
個人認証ＯＫ？
S73
NO
YES
データアクセス権確認ＯＫ？
S74
NO
YES
情報の閲覧、追加、修正又は加工
S75
閲覧、追加、修正又は加工の日時を付帯情報として付与
S76
情報の変更履歴を記憶
S77
情報の閲覧、追加、修正又は加工終了？
S78
NO
YES
END

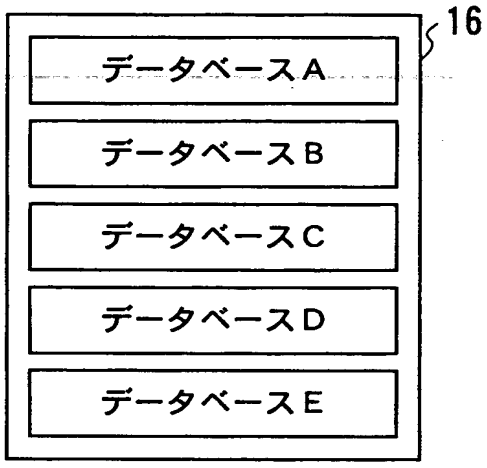
【図１７】


100
A
B
C
D
E
X
Y
Z
操作端末
操作端末
操作端末
操作端末
操作端末
出力装置
出力装置
出力装置
1g
2
3
4
5
6
11
12
13
14
15
16
17
18
個人照合手段
データアクセス権確認手段
データ改ざん防止手段
出力許可手段
制御部
データベース
日付日時付与手段
受信手段
21
31
41
51
61
自動送信手段
a2
b2
a3
b3
a4
b4
a5
b5
a6
b6

【図１８】


START
アクセス要求受信
S81
個人情報抽出
S82
個人認証ＯＫ？
S83
NO
YES
データアクセス権確認ＯＫ？
S84
NO
YES
情報の閲覧、追加、修正又は加工
S85
閲覧、追加、修正又は加工の日時を付帯情報として付与
S86
情報の変更履歴を記憶
S87
情報の閲覧、追加、修正又は加工終了？
S88
NO
YES
出力指示？
S89
NO
YES
出力許可確認ＯＫ？
S90
NO
YES
データ出力
S91
END

【図１９】



【書類名】　　要約書

【要約】

【課題】　本発明の課題は、種々の医療情報が記憶されるデータベースに対するセキュリティを向上させることである。

【解決手段】　管理サーバ１ａは、医療情報ＤＢ２の自動送信手段２１から送信される医療情報を、患者情報に基づいて患者毎に統合して管理し、この管理サーバ１ａに蓄積された医療情報を利用するためには、個人照合手段１２により、操作端末Ａ～Ｅの操作者の個人認証を行い、この個人照合手段１２により認証特定された操作者がアクセス可能な医療情報をデータアクセス権確認手段１３により確認した上で、医療情報へのアクセスを許可する。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　〔０００００１２７０〕

１．変更年月日　１９９０年　８月１４日
［変更理由］　新規登録
住　所　東京都新宿区西新宿１丁目２６番２号
氏　名　コニカ株式会社